HACKER JOURNAL

Anno 3 - N. 42
15 Gennaio 2004- 29 Gennaio 2004

Direttore Responsabile: Luca Sprea

I Ragazzi della redazione europea:
grand@hackerjournal.it, Bismark.it, Il Coccia, Gualtiero Tronconi, Ana Esteban, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Brugu s, Gregory Peron

Service: Cometa s.a.s.

DTP: Davide FO█ Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Eugenio Spagnolini

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Roto 2000

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.



HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. redazione@hackerjournal.it

## hack·er (hãk'∂r)

***"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."***

# SICURAMENTE INSICURI

**Gennaro ci ha mandato una mail che per noi merita l'editoriale. L'abbiamo riassunta per motivi di spazio, ma lasciando invariate le sue argomentazioni. Discutiamone.**

Si parla di sicurezza, di leggi che puniscono gli hacker e di buchi clamorosi in S.O. blasonati. Non si fa però mai cenno alle falle di sicurezza dovute a incuria e inesperienza (e incompetenza) di coloro che dovrebbero essere gli esperti. Pagati fior di quattrini e che spesso dovrebbero essere proprio loro a risarcire i danni alle società colpite, vista la loro imperizia.

A cosa servono i software per la scansione delle chiavi quando le password sono quelle preimpostate in fabbrica? Non mi è mai capitato di trovare un router ADSL su cui qualcuno si sia preoccupato di modificare la chiave di amministratore preimpostata in fabbrica, facilmente scaricabile e in bella mostra nel manuale in linea del router. Che magari è user: Admin e pw: Admin!

Ancor meno frequente è vedere qualcuno che si assicuri di dare agli utenti della rete accesso limitato ai soli servizi http e https. Poi, su richiesta del collega amico che deve scaricare l'ultimo album del suo cantante preferito, si aprono falle su tutto il sistema.

A proposito di peer to peer: quanto pensate che occorra a un manipolo di malintenzionati per creare una piccola rete p2p e che un software ad hoc per tale rete trasformi i pc delle vittime in proxy per dare ai malintenzionati una sicurezza di anonimato? Molto poco! Una decina di CD trendy e cinque o sei pc in rete.

Chi immagina di utilizzare un pc da rottamare come router/firewall tra due sottoreti della propria intranet in modo che una sottorete, magari aperta al pubblico, non possa accedere alla restante rete in cui sono registrati dati sensibili?

Quanti usano la possibilità di criptare intere parti dell'hard disk fidandosi ciecamente dell'antifurto installato (a cui non è stato modificato il codice di accesso preimpostato in fabbrica :-)? Abbiamo segnalato al servizio assistenza che sul nostro disco ci sono dati sensibili, per cui vanno prese determinate precauzioni in caso di sostituzione del disco stesso?

E se dal pollo arriva lo studentello sventolando un floppy, che chiede: "mi fa inviare questo testo al mio amico? Il mio modem si è rotto!"? Il pollo educatamente si sposta per non leggere la posta e lo studentello gli installa un trojan!

Quanti, dopo aver annotato una password su un foglietto, lo distruggono?

La notte chiudiamo il pc in cassaforte ignifuga, di giorno lo circondiamo di filo spinato. Eppure non abbiamo considerato che il Capo, portatosi il lavoro a casa, ignora che un'ora prima suo figlio dodicenne, attirato da una pubblicità ingannevole su un sito innocuo, ha infettato il pc del padre di virus che a loro volta hanno infettato il floppy su cui è stata scritta la relazione e di lì il pc del capo in ufficio.

Qualche apprendista stregone ha già pensato di far comprare al capo un portatile (tanto lui di soldi ne ha) e di aver messo in sicurezza la propria rete dimenticando che il collega a cui ha negato il p2p per scaricare l'ultima compilation di grido, rivolgendosi all'amico del cugino del cognato del fidanzato della figlia, si è fatto spiegare come installare un tunnel http.

Dobbiamo rassegnarci a tutta questa insicurezza?

Purtroppo sì! A meno che non si voglia tornare alle schede perforate (e qualche volta le rimpiango) oppure, molto più "semplicemente", lasciare fare ai veri esperti di sicurezza. Quelli che considerano la loro postazione uno strumento di lavoro e non un giocattolo e sono capaci di eliminare tutti quei servizi di cui non si ha bisogno, per vivere tranquilli e sicuri di essere insicuri :-)

**Gennaro Gaglione**

FREE HACK NET

HACKER JOURNAL

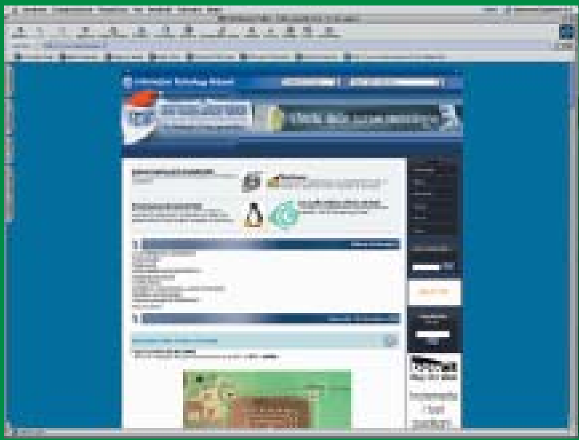
La prima rivista hacking italiana



## Nuove tecnologie al MAX

*Ciao! Mi chiamo Salvatore Aranzulla e gestisco un sito sui PC, sull'hardware e le nuove tecnologie in generale: MW Hardware MAX (http://www.hardwaremax.it). Potrei vederlo segnalato nella vostra [complimenti] rivista?*

*Salvatore Aranzulla*



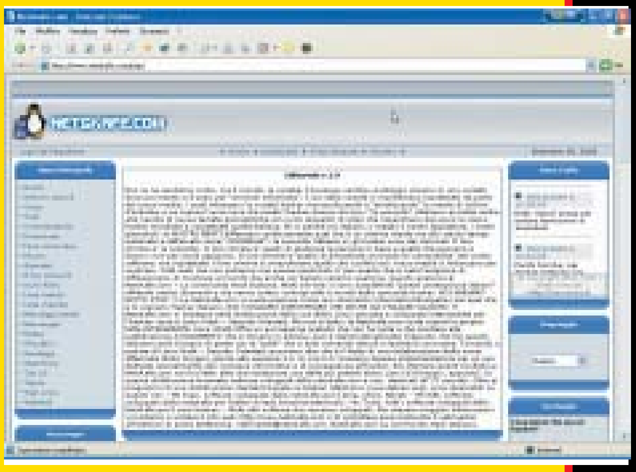
**Non lo so... ci dobbiamo pensare... forse sì, però... scherzo! Eccolo e complimenti a te!**

## STRISCIANDO LE NOTIZIE

*Salve, Sono il coordinatore del portale netskafe.com, chiedo, se è possibile, di recensire nella sezione news della vostra rivista il sito HTTP://WWW.NETSKAFE.COM, avente per scopo la realizzazione di una nuova distro linux orientata alla sicurezza informatica denominata LINUX HACK - SECURITY ORIENTED.*
*Attendo vostre notizie; cordialmente,*

*Giovanni Federico*

**Salve a te Giovanni!**
**Ora della distro lo sa tutta Italia. Mi sa che arriveranno presto rinforzi! Ciao e buon lavoro!**



## Nuova password!

**Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete gli arretrati, informazioni e approfondimenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo!**

**user: puffi**

**pass: buffi**

SECRETZONE

## Zio Bill il censore

*Colgo l'occasione per segnalarvi una "simpatica" interpretazione del film Matrix a http://www.tabletpctalk.com/pictures/comdex2003billg2.shtml. Anche se confesso di non aver mai pensato a zio Bill come ad un possibile Morpheus, ma si sa il potere della fantasia...*

*Darklady*



**Ci crederesti, che è stata censurata? Altro che Morpheus... lui combatte per la sua libertà. Zio Bill lo fa per altri scopi.**

04_05_HJ42_Posta 12-01-2004 18:17 Pagina 4

HACKER JOURNAL

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

## mailto:

redazione@hackerjournal.it

GOOGLEWHACK UNO

Ciao,
puoi spiegarmi meglio di cosa si tratta, ho letto su hacker journal [numero 40, Draghi di Google. N.d.B.], puoi farmi un esempio di come sia possibile trovarli? grazie…

**Gick**

***Ciao Gick, guarda qui sotto!***

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

GOOGLEWHACK DUE

A proposito di Googlewhack, che ne pensi di Menestrelli Sovrumani, oppure Armadilli Scontati, oppure Girogiostra Fulgente, oppure Sagrati Rampanti, oppure Incorporeità Incompresa? Li ho cercati in maniera tale da avere un suono decente, che potessero suonare come se li usassimo tutti i giorni. Spero li pubblicherete, è stato molto divertente!

**Bladefun**

***Li pubblichiamo sì, perché sono davvero carini!***
***A grande richiesta ripubblichiamo qui sotto una sintesi del testo del numero 40 dove Reed Wright spiegava il Googlewhack:***
***Un Googlewhack è una ricerca su Google, rigorosamente di due parole, che dà come risultato uno e un solo sito. Trovare Googlewhack non è difficile ma neanche facile ed è difficile fare esempi, perché nel momento stesso in cui si trova un Googlewhack è probabile che poco dopo non valga più, magari perché i risultati diventano due: il Googlewhack e la pagina di uno che segnala il Googlewhack, e cose così. Però nel momento in cui scrivo questo articolo "senectute immantinente" è un Googlewhack [lo è ancora. N.d.B.]. Ci sono delle regole: non vale usare le virgolette, le parole devono essere di uso comune (niente nomi propri, niente parole inventate) e il risultato non è valido se consiste nel link a una pagina di una lista di parole (come un dizionario o un glossario). Se trovate un Googlewhack lo pubblichiamo, sulla rivista o sul sito! E poi speditelo anche a www.googlewhack.com, dove li raccolgono. Qualche vero hacker sarà capace di scrivere un programmino Perl, o altro, che va in cerca di Googlewhack. Lo aspetto al varco!***
***Vale ancora. Chi trova Googlewhack belli come questi, o di più? Qualcuno è capace di fare il programmino? Chi scopre le varianti del gioco? Siamo qua!***

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

REGEX UNO

Non ho capito bene cosa siano queste espressioni e come possano essere utilizzate. Vorrei anche chiederti dove posso trovare documentazione buona su queste cose e soprattutto di come si possano implementare in Java.

**Daniele.**

***Per il momento mi limito a dirti di fare una ricerca su Google della parola regex e di visitare, per Java, http://regex.info. Poi, leggi qui sotto. :-)***

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

REGEX DUE

Ciao, […] ho trovato la semplice soluzione del secondo caso, ma mi riesce difficile trovare quella per il terzo e mi sorgono alcune domande: non c'è un'istruzione che non dà dei parametri come [0,9] ma dice "prendi il pezzo della stringa fino a che trovi il carattere…"?

**LoRd_MoRo**

***Ciao, guarda qui sotto!***

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

REGEX TRE

Ciao Barg,
Ti scrivo perché [complimenti] il tuo articolo sul #40 […] rispondo alle tue domande: […] Comunque volevo farti anche una precisazione sul 1° problema da te risolto... in realtà la tua soluzione \d{2}\d?\d?[/.;@#-]?\d{5}\d?\d?\d? è sì in grado di riconoscere tutti i numeri di telefono italiani validi, ma non SOLO i validi […] il mio problema è molto semplice: estrarre tutte le Email di una certa "cartella" da Outlook Express in modo da salvarle in un formato diverso [eml, doc, xml, html, …). […] non mi era venuto in mente che avrei potuto scrivere io il tool in questione usando java con JLex e Cup… sono proprio pigro! ;-)

**Jerk**
**jerk@hackerjournal.it**

***Ciao Jerk!***

***Ho molto riassunto la tua mail e quelle prima (compresi tutti gli altri che hanno scritto, da Roberto Bossola in poi) perché qui nella posta non abbiamo spazio a sufficienza per approfondire la questione. Ma è per dire che lo farò in un prossimo articolo, con tutto lo spazio che serve e con tutte le vostre soluzioni, proposte e domande. Il tema delle espressioni regolari è piaciuto e d'altronde l'articolo era a livelli elementari, quindi non poteva entrare nel merito di tutto. Si può dire molto di più e… lo faremo. Se qualcuno ha domande in merito si faccia pure avanti!***



- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

COME DIVENTARE HACKER

Vi scrivo per chiedervi come è possibile diventare un "hacker" (intendo un esperto di computer, non uno che rompe le scatole agli altri). Ho il mio primo pc da 4 mesi e ho comprato praticamente ogni tipo di rivista. L'impressione che se uno non ne sa non ne dovrà mai sapere mi è venuta dopo la prima pagina. Imparare a usare il pc senza sapere l inglese non e certo facile e complicare l'italiano con termini cifrati non mi aiuta, lo devo buttare? Posso trovare un manuale base con

dizionario? Voi cosa consigliereste a un alieno appena arrivato in questo mondo che vorrebbe usare un pc? Vi ringrazio anticipatamente per la pazienza sperando in una risposta positiva.



**Alessandro**

***Caro Alessandro,***
***non so da dove cominciare ma ci provo. Sono usciti numerosi libri negli ultimi mesi con titoli tipo "Il manuale del giovane hacker" e simili, ma non ti aiuteranno. L'hacker non compra un libro per diventare hacker; curiosa, si impegna, studia, prova, improvvisa, inventa fino a quando non può scriverne uno! Scherzo, ma non completamente. Sii curioso e cerca di andare sempre alla sostanza e al cuore delle cose e metà del lavoro l'hai fatta. Un esempio stupido ma per me coerente: che cos'è un byte? Un hacker si butta su it.wikipedia.org e trova la risposta. Un non hacker cerca un libro scritto da un hacker che lo spieghi… e ora tutta la verità, fino in fondo. L'esempio che ti ho fatto funziona anche in italiano. Ma l'inglese è indispensabile, non solo per fare l'hacker. Un consiglio: non prenderla come una lingua da imparare, ma come una sfida da affrontare. Scriviti tre, cinque, dieci vocaboli di inglese al giorno e imparali a memoria, ogni giorno tre/cinque/dieci vocaboli nuovi. Tempo sei mesi e ci darai lezioni a tutti. Quando sei in dubbio, scrivici.***

- - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - -

## FORSE TROPPO CONTROLLO

Gentile redazione,
volevo chiedervi, siccome da poco ho comprato un secondo pc per i miei figli, come poter controllarlo dalla mia macchina, e come loggare i siti da loro visitati, i programmi installati, i tasti digitati eccetera, e inviare tutto alla mia mail. Poiché non sono un esperto di linguaggi vi prego di indicarmi dei programmi per poterlo fare automaticamente. (La sicurezza passa anche di qua: vedere cosa fanno i propri figli col computer e quali siti visitano).

**Peppe**

***Gentile Peppe,***



***potrei consigliarti decine di keylogger (i programmi che loggano i tasti premuti) e altri programmi che fanno le cose che vuoi tu, ma non lo faccio, per due motivi. Primo: seguendo Hacker Journal e Hacker Magazine avrai già in casa un arsenale di software e di istruzioni. Secondo: penso che saresti molto più sicuro parlando con i tuoi figli, navigando insieme a loro e fidandoti. Pur sapendo che gli capiterà di sbagliare, e che sbagliare significa crescere. Non fosse altro che, se loro ne sanno più di te, tutti i tuoi keylogger risulteranno vani.***

- - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - -

## INTERCETTAZIONE GSM

Sono uno studente di ingegneria delle telecomunicazioni e vorrei sapere se conoscendo l'identificativo IMEI e/o il numero telefonico di telefonino sia possibile attraverso la rete e eventualmente con qualche altro apparato riuscire a localizzarlo (anche a breve raggio) o sapere il traffico in entrata e uscita.

**Lastangel83**

***Vedo poche possibilità.***
***L'IMEI non ti serve a niente per la pura localizzazione (al massimo è meglio avere uno scanner radio per captarne il***



***segnale quando chiama). Per quanto riguarda l'ascolto del traffico, non ti serve sapere l'IMEI quanto invece l'IMSI, immagazzinato sulla SIM, che contiene le informazioni dell'abbonato. A livello accademico il codice di cifratura GSM è stato violato, ma a livello di utilizzo pratico non è esattamente facile***

- - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - -

## WINDOWS 98 A TEMA

Ciao! […] Mi chiedevo se esiste un metodo o un programma per "emulare Windows XP" su Windows 95/98 in modo tale […] da far assomigliare il desktop a quello di Windows XP, cambiare l'aspetto delle finestre e della barra delle applicazioni e il menu d'avvio… In pratica usare Win 95/98 con le caratteristiche grafiche di XP.

**attashow**



***Ciao a te!***
***Puoi tranquillamente trovare un sacco di temi come quello che cerchi nei siti dedicati, per esempio http://www.aaa-themes.com/xpdesktopthemes.phtml. Stai attento ai siti che ti regalano il tema ma poi non ti mollano più e vogliono a tutti i costi una marea di dati per inviarti mail pubblicitarie.***

- - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - -

## POSTA DEL KAISER

cara redazione so gia che le mie parole non vi faranno minimamente riflettere comunque continuero nel mio intento che qualche cosa cambi. […] xke no cambiare nome alla rivista e chiamarla securitycomputerjournal siccome la state facendo diventare una rivista di sicurezza. […] x me i virus sono il tramite tra massmedia e l'hacker. […]
Poi la rivista è carina (si fa x dire) mancano troppe robe, guide al linguaggio c++, c, pascal, vb, ecc… in pratica programmazione, magari aggiungere sorgenti di programmi, virus (non quella sotto specie del primo numero), cosi che il lettore possa confrontarlo con i suoi sorgenti. Nella rivista mettere + hacker e - sicurezza […]
Ultime precisazioni il vostro sito fa schifo […]
Avrei piacere che ritoccaste questa lettera e la pubblicaste sul prossimo numero di hj con risposta inclusa. […]
ciao by



**kaiser741**

***Ciao kaiser!***
***Abbiamo sintetizzato la tua lettera, non***

# HOT!

## CISCO VULNERABILE SUL WI-FI

**Cisco, monopolista di fatto del mercato dei router,** ha ammesso recentemente una vulnerabilità nella sua linea di punti di accesso wireless Aironet che può consentire ad aggressori ben motivati di accedere a una rete aziendale e curiosare oltre il lecito. Il problema sta nelle chiavi di cifratura, che vengono trasmesse in modo wireless e in testo non cifrato: quindi chiunque, dotato di un computer e dell'antenna giusta, può intercettare le chiavi stesse. una volta che un aggressore è in possesso delle chiavi, qualunque cifratura è inutile per proteggere i dati. La vulnerabilità affligge i modelli delle serie 1100, 1200 e 1400 con software Cisco IOS 12.2(8)JA, 12.2(11)JA e 12.2(11)JA1. Gli amministratori di rete possono risolverla, tra l'altro, aggiornando a IOS versione 12.2(13)JA1 o successivo. Certo che se gli aggiornamenti fossero numerati in modo più umano anche le vulnerabilità avrebbero vita più difficile!

---

## SUN ATTACCCA MICROSOFT CON JAVA LOW-COST SU LINUX

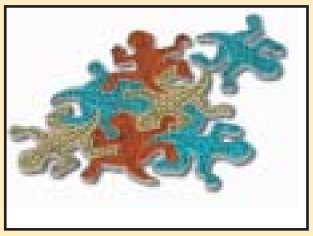
**Nell'intento di togliere quote di mercato a Windows nel mondo aziendale,** Sun ha abbassato il prezzo del suo Java Enterprise System a 50 dollari l'anno per utenza e ha portato Java Desktop System, che consente di collegarsi a un ambiente Windows da una interfaccia interamente basata su Linux con Star Office e Ximian, a 25 dollari per utenza per anno, il tutto fino a metà 2004.
La mossa segue il successo conseguito da Sun in Cina, dove un accordo con China Standard Company, azienda controllata dal governo cinese, apre la strada letteralmente a centinaia di milioni di computer sui quali verrà installato Java Desktop System e non Windows.

## MAI PIÙ SEDIE A ROTELLE



**All'università Waseda di Tokyo,** in collaborazione con la produttrice di robot Tmsuk, i ricercatori hanno messo a punto un prototipo di robot capace di camminare su due gambe meccaniche e contemporaneamente trasportare una persona seduta. Si può immaginare come un progresso di questo tipo spalanchi la porta a un futuro assai più confortevole per i disabili e gli ammalati.
Il prototipo si chiama WL-16, è alimentato a batterie e riesce a spostarsi in avanti, all'indietro e lateralmente reggendo un adulto del peso massimo, per ora, di sessanta chili. Secondo Yoichi Takamoto, amministratore delegato di Tsmuk, per arrivare a un modello realizzabile in serie ci vorranno "almeno due anni". Nel frattempo, però, il robot è già capace di mantenere l'equilibrio quando il suo carico umano si sposta e riesce a fare passi lunghi trenta centimetri. Prossimi obiettivi: renderlo capace di fare le scale (per ora il gradino massimo superabile è alto pochi millimetri) e passare dall'attuale radiocomando a un joystick montato a bordo, utilizzabile dal passeggero.

## UN PUZZLE DA VERI HACKER



**Mille pezzi, cinquemila pezzi, settemila pezzi sono roba da niente.** Pensate a un puzzle dove i pezzi hanno tutti forma uguale e ci sono miliardi di incastri possibili ma una sola soluzione corretta.
È il principio dello Shmuzzle, gioco inventato da tale Sam Savage, già docente di Management Science alla Università di Chicago. Savage ha avuto l'idea osservando alcune opere di Maurits Cornelis Escher, artista olandese morto nel 1972 e autore di lavori che nascondono trame geometriche assai intricate e paradossi della prospettiva che lasciano interdetti. Escher era un maestro della tassellatura, l'arte di riempire completamente un piano con figure che si incastrano l'una nell'altra all'infinito, senza lasciare spazi vuoti. E da un'opera di Escher intitolata Reptiles è nata l'idea di creare un puzzle dove lo scopo è sempre quello di comporre il disegno, ma i pezzi hanno tutti forma uguale. Invitiamo tutti a fare un salto su http://www.shmuzzles.com, dove è anche possibile provare l'ebbrezza di un puzzle davvero impossibile direttamente da browser. Il vero hacker si fermerà anche a considerare i principi geometrici che stanno dietro al lavoro, magari aiutandosi con http://www.shmuzzles.com/formula.htm.

## LE MAPPE PIÙ BELLE



**Sono numerose le iniziative di mappatura di Internet in forma grafica, ma quella adottata da Opte.org per il momento è certamente una delle più suggestive.** Anche una delle più veloci, dal momento che uno degli obiettivi del progetto è produrre mappe accurate in un solo giorno con un solo computer, là dove altri progetti impiegano mesi per arrivare a un risultato. L'idea è il classico uovo di Colombo: disegnare un diagramma di Internet semplicemente usando un comune tool di manutenzione di rete locale, ma estendendo il rilevamento a tutta la Rete. E così il progetto si appoggia fondamentalmente a traceroute, uno dei programmi più comuni per il rilevamento dei percorsi attivi su Internet. Il progetto Opte necessita di ulteriori perfezionamenti. Per esempio le mappe sono centrate su un singolo punto e quindi non sono presenti tutti i percorsi che da quel punto non passano. Altro problema è la limitazione del rilevamento agli indirizzi di classe C per ridurre il tempo necessario alla scansione. Ciononostante le mappe di Opte ci piacciono alla follia e speriamo riescano a perfezionarle senza che ne risenta il loro fascino. Da quando esiste Internet, infatti, sono la cosa più simile a una rete neuronale come quelle presenti nei nostri cervelli.

## COLPA DELL'ADMIN

**Molti exploit hackeristici sono dovuti a cattivo monitoraggio delle reti da parte degli amministratori.** È l'opinione di Bryan Satin, technology director presso la società specializzata nella fornitura di servizi di sicurezza Ubizen, espressa in una recente intervista a VNUnet.com.
Nelle loro indagini postmortem, che seguono un attacco a una rete o a un sistema amministrativo, il più delle volte emergono trascuratezza e mancanza di aggiornamento, fattori che hanno portato il numero di incidenti a quadruplicare (da 20 mila a 80 mila) tra il 2000 e il 2003.
La maggior parte delle violazioni avviene attraverso un server Web e quasi sempre usando gli stessi exploit, come backdoor Web-based – root.exe e cmd.asp – oppure usando a scopo ostile strumenti altrimenti utilissimi per la sicurezza dei sistemi, come iroffer.exe. Secondo Satin gli hacker sono anche divenuti molto più bravi di un tempo a nascondere le loro incursioni. Tempi duri per gli amministratori di rete!

## JON HA VINTO ANCORA !



**"Dvd Jon", che nel 1999, a 15 anni ha scritto il software in grado di sproteggere i DVD,** e che trovate in rete con il nome di DeCSS, è stato assolto anche in appello dall'accusa di avere violato la legge norvegese di protezione del copyright. Era suo diritto, ha stabilito la corte, realizzare un programma capace di fargli vedere sul proprio PC i DVD che aveva regolarmente acquistato, anche se questo ha eluso le difese poste a protezione dei DVD. Una bella sconfitta per le grandi multinazionali dell'intrattenimento video e musicale, che contavano in una condanna esemplare (una pena carceraria e qualche migliaio di Euro di multa) che ponesse argine a tutto ciò che alla base potrebbe minare i loro plurimiliardari affari. Lo scossone potrebbe essere definitivo e comunque convincere anche altri settori a porsi in altri termini il problema delle copie illegali di CD e DVD. Ovvero se non sia meglio ripensare alla politica di distribuzione e commerciale, così da renderli realmente accessibili a tutte le tasche, scoraggiando sul nascere le necessità stesse di protezione. Anche perché è evidentemente una battaglia fallita in partenza: dove c'è una protezione, ci sarà sempre qualcun altro che tenterà di scardinarla. Nella foto il giovane Jon Johansen.

## CHE BELLO LAVORARE ALLA NASA



**Pare che l'Agenzia spaziale americana sia stata dichiarata "miglior posto in cui lavorare dentro il governo federale".**
Evidentemente, con le minacce di terrorismo che imperversano, è meglio lavorare guardando le stelle che non il terreno, o peggio le proprie spalle...

Un'ombra di 500 chilometri si stende sull'Antartide per via di un'eclisse e chi la studia fa il più bel lavoro nel governo USA.

# HOT!

## UN HOTSPOT IN OGNI BIBLIOTECA.. MA IN INGHILTERRA

**Il ministro inglese Stephen Timms** ha aperto il lavori di un convegno su Wi-Fi & 3G confermando che va avanti il piano di installazione di un punto di accesso wireless in ogni biblioteca pubblica del Regno Unito, annunciato lo scorso settembre.
Si spera che i nostri governanti, se non sanno fare meglio, almeno siano in grado di scimmiottare i colleghi britannici.

---------------------------------------

## BLUE SHIRT OF DEATH

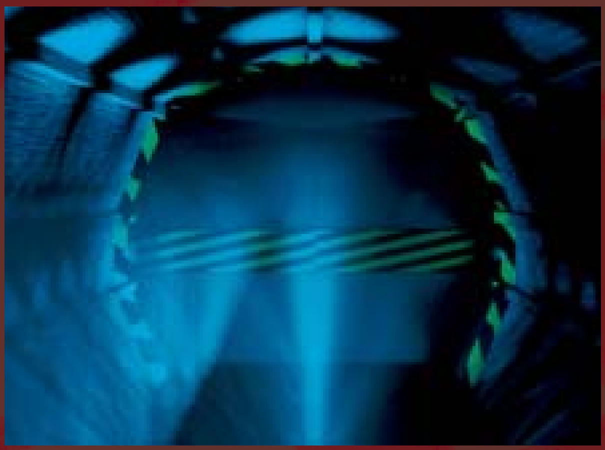
**È inutile; se si è geek, si hanno magliette a dimostrarlo (chi non sa che cosa sia un geek, continui a leggere Hacker Journal e lo diventerà).** A ErrorWear lo hanno capito e hanno realizzato splendide t-shirt che riproducono tutti gli errori di sistema possibili e immaginabili, per Windows, per Mac, per Unix, per i computer più vecchi, in ogni circostanza. E siccome i geek sono tutt'altro che stupidi hanno realizzato le t-shirt sia per maschietto che per femminuccia, con il giusto taglio per ognuno.
Dei prezzi non vale neanche la pena di parlare: davanti a magliette così non si discute! Al massimo, si resetta.

**http://www.errorwear.com**



# PORTE, CAVALLI

**Ci sono più cose in cielo e in Terra, Orazio, di quante ne possa sognare la tua filosofia – Shakespeare, Amleto, atto I, scena V "Ci sono più porte aperte nel tuo computer,**



**Lascia perdere quelle sciocchezzuole come seriali, parallele, USB;** le vere porte del computer sono quelle logiche: i percorsi sui quali si svolge lo scambio dei dati tra programmi, servizi, accessori hardware, siti e, purtroppo, attacchi ostili. Le porte logiche a disposizione di un computer odierno sono ben 65.536 e si dividono essenzialmente in porte conosciute e porte ignorate. Le porte conosciute sono le prime 1.024 e sono associate ai servizi di sistema; le porte ignorate sono tutte quelle che seguono, dalla 1025 in poi e che sono normalmente associate a servizi non identificati, ovvero non facenti parte del sistema stesso. Purtroppo, a parte alcuni utilizzi più che legittimi, questi "servizi" spesso consistono in virus, worm e cavalli di Troia. I virus sono programmi che si autoreplicano e si diffondono usando altre applicazioni all'interno del computer ospite. I worm funzionano come i virus, ma si propagano attraverso la rete. I cavalli di Troia sono applicazioni che mascherano, sotto l'apparenza di un programma utile, un codice dannoso che può svolgere svariate attività all'interno del computer.

## Le note tra le ignote

**Vediamo ora nel dettaglio le più "note" fra le porte non note e i pericoli che possono rappresentare.** Come noterete, all'inizio dell'elenco vi sono anche alcune porte inferiori alla 1024, che però possono essere usate in modo fraudolento da programmi diversi da quelli per cui sono state pensate e riservate.

### Porta 21, 5400
Software come Blade Runner, FTP trojan, Invisibile FTP, WinCrash usano la porta 21 per creare varianti pericolose del servizio FTP; queste varianti possono essere controllate in remoto e permettono l'upload o il download di file e programmi.

### Porta 23
Viene a volte usata dal servizio TTS, che funziona come un programma di emulazione terminale operante in maniera invisibile (un server telnet nascosto). Una volta connessi in modalità telnet classica diventa possibile impartire comandi da eseguire sul sistema colpito.

### Porta 25, 110
Se non state usando programmi per la posta, ma vedete aperte queste porte, c'è qualcosa che non quadra. È possibile che un daemon ben nascosto dentro una simpatica animazione Flash o uno screensaver che mostra immagini di donnine allegre stia cercando di rubare password di sistema e di spedirle via email.

### Porta 31, 456, 3129, 40421
Servizi come Hackers Paradise usano soprattutto la porta 31 per usurpare il controllo del sistema e modificare il registro di configurazione.

### Porta 41, 2140, 3150, 60000
Un daemon noto col nome di Deep Throat offe enormi possibilità di gestione remota del PC, fra le quali server FTP, amministrazione remota, cattura schermo e gestione dei processi in esecuzione.

### Porta 113
Il servizio Kazimas è un worm che si diffonde attraverso mIRC. Una volta infettata la macchina, si replica e modifica il file di impostazioni del mIRC stesso.

### Porta 119
Happy 99 sembra un innocuo passatempo a base di fuochi d'artificio, ma in verità nasconde un pericolosissimo programma di trafugamento password, mail spamming e attacchi DoS.

### Porta 555, 9989
Programmi come NeTAdmin e Stealth Spy hanno come scopo quello di distruggere il sistema infettato dopo essersi riprodotti e distribuiti.

### Porta 1010, 1015
Il servizio noto come Doly Trojan è un cavallo di Troia capace di acquisire completamente il controllo remoto del PC infettato.

### Porta 1024, 31338
Il servizio NetSpy è uno dei più noti in grado di spiare l'attività all'interno di un PC e di gestirla in remoto. Può anche bloccare il pulsante Start e nascondere la barra delle applicazioni.

### Porta 1234
Il daemon Ultors è un altro trojan in grado di far acquisire il controllo remoto della macchina infettata.

### Porta 1600
È associata a un trojan di concezione molto semplice, il Shivka-Burka, che ha solo funzionalità di trasferimento file.

### Porta 1999
Il servizio BackDoor è stato uno fra i primi cavalli di troia con associata una backdoor. Offre svariate possibilità di controllo remoto del PC come controllo del mouse, video,

# E DAEMON



caro mio, di quante puoi fare in tempo a controllare senza un buon programma" - anonimo in incognito

task, chat e messaggistica.

**Porta 2115**
Bugs è un programma di accesso remoto che consente la gestione dei file e l'esecuzione di comandi.

**Porta 2155, 5512**
Il daemon Illusion Mailer è un programma di spamming di posta elettronica che consente di inviare messaggi usufruendo dell'identità della vittima.

**Porta 2565**
Il servizio Striker, associato a questa porta, ha come unico intento quello di far fuori Windows. Dopo il riavvio comunque non rimane residente in memoria e pertanto se l'attacco viene evitato, non si corrono rischi futuri.

**Porta 2583, 3024, 4092, 5742**
Un cavallo di troia noto col nome di WinCrash sfrutta queste porte per insediarsi e per compiere la sua azione. Essendo dotato di strumenti come il flooding, è considerato uno strumento potente e pericoloso.

**Porta 2600**
Il daemon RootBeer è un cavallo di Troia dotato di accesso remoto con le seguenti caratteristiche: messaggistica, controllo finestre, controllo monitor, controllo audio, controllo modem, congelamento del sistema.

**Porta 2989**
Il servizio RAT è un cavallo di Troia a backdoor progettato per distruggere il contenuto dei dischi rigidi di sistema.

**Porta 3459, 3801**
Il daemon Eclipse è un servizio FTP invisibile che conferisce accesso al trasferimento dei file ed alla loro esecuzione, cancellazione e modificazione.




**Porta 4567**
Il servizio File Nail è una backdoor remota associata ad ICQ.

**Porta 5001, 30303, 50505**
Il virus Sockets de Troie è un programma che si diffonde come una backdoor di amministrazione remota. La sua istallazione coincide con un errore DLL e, dopo essersi istallato nella directory \windows\system, modifica le chiavi del registro di configurazione.

**Porta 6400**
Il daemon tHing ha la sua pericolosità non tanto nella sua attività intrinseca, ma perché viene sfruttato da virus come metodo di infezione di altre macchine.

**Porta 7000**
Il daemon Remote Grab è in grado di catturare schermate del monitor remoto, in modo tale da avere una visione esatte delle attività svolte.

**Porta 10101**
Il cavallo di Troia BrianSpy è dotato di tutte le classiche funzionalità di questi programmi, con l'aggiunta di un servizio grazie al quale riesce a eliminare i file di scansione degli antivirus istallati.

**Porta 12223**
Il servizio che sfrutta questa porta è un KeyLogger che ha la possibilità di inviare in tempo reale al cracker tutta l'attività svolta sulla tastiera del PC remoto.

**Porta 12345**
Forse la più nota tra le porte non note: è la porta a cui risponde il server della backdoor NetBus, ormai vecchiotta ma ancora in grado di creare danni.

**Porta 20000**
Il trojan Millennium è un programma scritto in VB che offre come caratteristiche: controllo file, controllo CD-ROM, controllo barra applicazioni, controllo audio, prelievo password, controllo browser, riavvio del sistema.

> **un daemon, non un demone**
>
> **I traduttori da spendere poco leggono daemon e dicono demone.** In realtà il daemon è un essere soprannnaturale a metà tra l'umano e il divino, come una sottodivinità oppure il fantasma di un grande guerriero morto, comunque sia non necessariamente buono o cattivo. Il demone, invece, è una creatura intrinsecamente malvagia, che può possedere gli umani.

**Porta 22222, 33333**
Il cavallo di Troia Prosiak è l'ennesimo daemon di controllo remoto che offre il classico arsenale di funzioni tipiche di questa categoria di programmi.

**Porta 31337, 54320**
Il daemon Back Orifice è un programma altamente pericoloso che sta alla base della concezione di sviluppo di altri Trojan per Windows.

## Prudenza

Per un cracker avere libero accesso alle porte è un fattore di vitale importanza per scatenare i suoi attacchi. Questo elenco di porte e di servizi associati deve servire come stimolo all'autoprotezione. Un buon firewall, pur magari non essendo la soluzione a tutti i mali, impostato nei limiti del possibile con delle regole abbastanza ferree sulla possibilità di utilizzare determinate porte, può certamente limitare le strategie di ingresso nel PC da parte di estranei.

CAT4R4TTA
cat4r4tta@hackerjournal.it

# HAI SEGUITO O

Un pedinamento non funziona come si vede nei film ma è ben più complesso.

**Solo i paranoidi sopravvivono, ha detto una volta Gordon Moore, il fondatore di Intel. Ugualmente, solo i paranoidi considerano la possibilità di essere pedinati.** Eppure, in un Paese come il nostro, dove il numero di intercettazioni telefoniche pro capite è secondo solo a quello degli USA, la possibilità che qualcuno ci segua, per quanto remota, non è da escludere.

Per questo ho pensato di spiegare un po' come funziona la faccenda. Certe manovre e certi atteggiamenti sono inconfondibili e conoscerli aiuta ad accorgersene.

### > Lavoro di squadra

**Dimenticate i film: il pedinato inseguito dal pedinatore è una stupida semplificazione.** Un vero pedinamento è un lavoro di squadra, compiuto da un team affiatato. Un singolo pedinatore è troppo a rischio di venire scoperto e di perdere il contatto. Le situazioni che vedono un solo pedinatore sono al limite, quando non c'è proprio altro da fare o bisogna osservare la massima discrezione.

## >> I metodi di sorveglianza

**Le tecniche di sorveglianza sono fondamentalmente cinque: a piedi, mobile, statica, tecnica e combinata.**

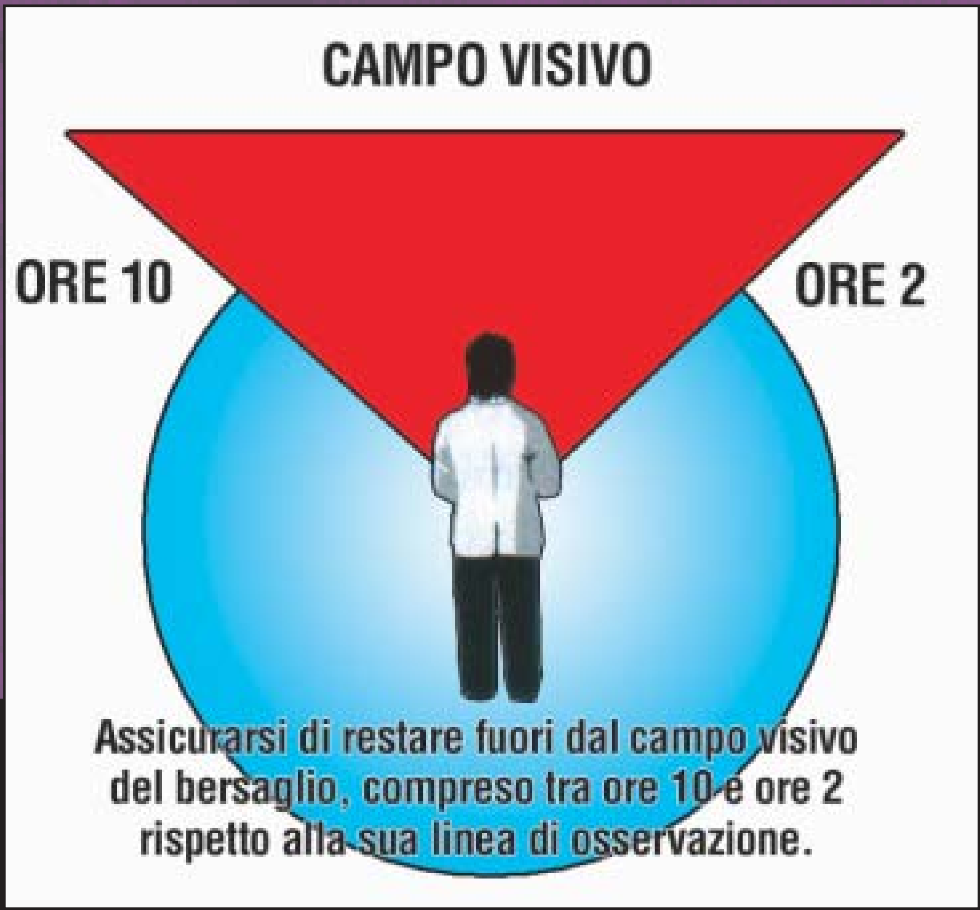
### > A piedi

**Un pedinamento professionale è preparato in anticipo, con una certa idea di dove si recherà il bersaglio e di quale sarà il percorso, e ricognizioni preparatorie del terreno.** Quando è possibile, la maggior parte del pedinamento viene svolta a piedi, perché è la tecnica che frutta le informazioni migliori. Il pedinamento automobilistico è solo un espediente per stare dietro al bersaglio intanto che si sposta in macchina ed è solo quando il bersaglio finalmente parcheggia che si ricomincia a raccogliere informazioni. Naturalmente il pedinatore è pronto a qualunque variante e, per esempio, avrà pronta in vicinanza una bicicletta se non addirittura i pattini in borsa (non in Italia, dove ti guardano strano da subito).

**I team di pedinamento stanno attenti a evitare due cose: farsi vedere troppo spesso dal bersaglio e comportarsi in modo insolito.** Questa combinazione di problemi porta alla necessità, come si è detto, di essere organizzati in squadra, i cui componenti sono in contatto in modo non evidente, per esempio tramite radio nascoste.

### > In movimento

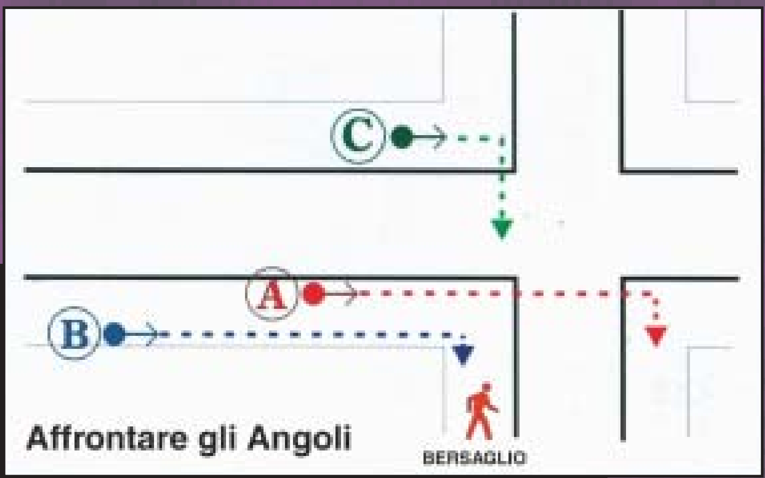
**La sorveglianza mobile è dove si capisce subito che una persona sola non basta.** Se siamo seguiti in motorino, in auto, in barca (succede!) basta un minimo imprevisto a seminare un singolo



Assicurarsi di restare fuori dal campo visivo del bersaglio, compreso tra ore 10 e ore 2 rispetto alla sua linea di osservazione.

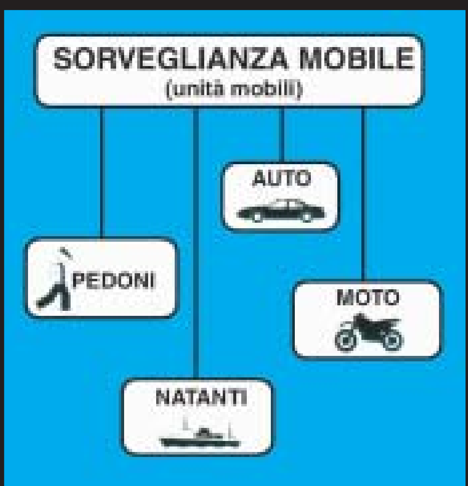
# S'EI SEGUITO?

**Che siate il bersaglio o il pedinatore, ecco qualche trucco da sapere...**




pedinatore. Quindi il team si muove a bordo di più veicoli, differenziati, e il contatto continuo, probabilmente via radio, è essenziale, per riferire osservazioni sul bersaglio, condividere informazioni, registrare dati e nel contempo non causare incidenti, che sono la cosa peggiore in assoluto per un pedinatore mobile.

**In qualsiasi momento un pedinatore mobile è pronto a trasformarsi in pedone o saltare su un autobus.** Per seminare un pedinatore motorizzato la cosa migliore è parcheggiare in un'area ad altissimo rischio di multa o rimozione forzata. L'ultima cosa che può permettersi il pedinatore, ricordate, è attirare l'attenzione o essere in qualche modo schedato da polizia o vigili urbani…




## > Sorveglianza statica

**Un pedinatore statico osserva da fermo, da una macchina, un edificio, un tetto, un bar, o anche dal marciapiede.** Ci sono diversità fondamentali tra il pedinamento nelle aree urbane e quello nelle campagne, ma in ambedue i casi la sorveglianza può essere di lungo termine (tutti i giorni, negli stessi orari…) o breve termine (oggi e mai più).

**I luoghi caldi sono i parcheggi, i cancelli, i portoni, in pratica tutti i luoghi dove inizia o termina un pedinamento.** Per un pedinatore la posizione più comoda è osservare da un'auto parcheggiata proprio di fronte all'obiettivo. Ma ovviamente è facile essere individuati e quindi, più probabilmente, verrà scelta una posizione relativamente nascosta, a un angolo di strada, o dietro una siepe, o a fianco di un grosso camion. Tenete presente che si rischia di essere scoperti anche quando si cerca di nascondersi troppo bene; una persona che sbircia da dietro una siepe viene notata subito dai passanti. Per cui il pedinatore è nascosto ma non troppo.

**Sul breve termine l'osservazione viene svolta anche a piedi approfittando di cabine telefoniche o fermate degli autobus,** o altri posti dove è plausibile che una persona sia ferma per un tempo relativamente lungo. Il sorvegliante statico difficilmente si trasforma in dinamico, a seguire il bersaglio; di solito funge da interruttore del pedinamento, che avvisa la squadra dell'individuazione del bersaglio e attiva i sorveglianti mobili, o conferma previsioni di percorso ("come previsto è entrato in ufficio").




## > L'ausilio della tecnica

La tecnologia è strumento sempre più usato nelle operazioni di pedinamento. I dispositivi impiegati sono prevedibili:

- **radiomicrofoni (a lunga distanza o cimici installate in loco)**
- **microfoni convenzionali e registratori**
- **intercettazioni telefoniche**
- **videoregistrazione**
- **tracciamento veicoli tramite GPS o compilazione manuale di mappe secondo le informazioni ricevute nel corso del pedinamento**
- **intercettazioni informatiche**

Ognuno di questi strumenti ha forti limi-

# PEDINAMENTI

tazioni ma, usato nel modo giusto, è un'arma potente per raccogliere informazioni e fornire appoggio tecnico e tecnologico ai pedinatori in carne e ossa.

## > Sorveglianza combinata

**I pedinamenti più efficaci (e più pericolosi per il bersaglio) sono quelli in cui viene assemblato un team apposito e vengono pianificate a tavolino tutte le risorse da impiegare, per situare il mezzo e la persona appropriata nel luogo e nel momento più opportuni.** Se tutto è previsto, è difficile evitare un pedinamento; magari ci si dirige in una zona pedonale per evitare una macchina, ma a bordo c'è un pedinatore in più che scende immediatamente. Il veicolo parcheggiato davanti a casa potrebbe cambiare ogni giorno, ruotando tra due o più auto o tra un'auto e un furgone e via dicendo.

## > Salta la copertura

**Dal suo punto di vista il pedinatore è come un gatto, o come l'eroe di un videogioco: ha un numero limitato di "vite", ossia di situazioni in cui può esporsi senza essere sospettato, dopo di che la sua intenzione diventa palese e si ritrova "bruciato".** Per questo i team organizzati definiscono anticipatamente un livello di rischio accettabile, che dipende dalla consapevolezza del bersaglio e dalle circostanze in cui avviene il pedinamento. Per fare esempi banali ma evidenti, se il bersaglio entra in un bar è troppo rischioso entrare e prendere un caffè al suo fianco. D'altro canto, se il soggetto entra in un ipermercato con più uscite e più piani è praticamente inevitabile che verrà seguito. In linea di massima un pedinatore cercherà di evitare di entrare nello stesso locale del bersaglio e, se il bersaglio ha una strategia di elusione, è in quel momento che deve metterla in atto.

## > Da guadagnare e da perdere

**Successo e insuccesso di un pedinamento dipendono da che compromesso verrà scelto tra l'avvicinarsi al bersaglio e tutelare le "vite" dei pedinatori.** Avvicinandosi molto si ottengono le maggiori informazioni ma si perde il maggior numero di "vite". Ogni incontro ravvicinato con il soggetto è, per il pedinatore, una enorme opportunità e un enorme rischio. Molti team di pedinamento usano parlare in termini di temperatura, come se il bersaglio fosse una fonte di calore. Il contatto migliore (e rischioso) è quello rovente, mentre un pedinatore che osserva con un cannocchiale dall'alto di una terrazza nascosto tra le piante è decisamente freddo.




**Un pedinatore esperto sa quando è a rischio e si rende conto del fatto di essere stato individuato.** È anche capace di scegliere al volo se conviene rischiare, se passare il bersaglio a un altro membro del team o se mollare tutto per non insospettire ulteriormente il bersaglio. Sono situazioni in cui la risposta globale del team alla situazione consente spesso di accorgersi con certezza dell'esistenza di un'iniziativa di pedinamento.

**Quali sono i pedinatori migliori, da cui occorre stare alla larga il più possibile?** Paradossalmente, e purtroppo, i veri professionisti sono le persone più grigie e invisibili che esistano, su cui un inesperto non scommetterebbe un centesimo. Più una persona salta all'occhio meno è probabile che faccia parte di un team di sorveglianza. La regola fondamentale di un pedinamento è finire il meno possibile nel campo visivo di un bersaglio, compreso tra ore 10 e ore 2 rispetto alla direzione in cui questo guarda. I team bene organizzati fanno in modo da evitare l'area del campo visivo e, se proprio si deve essere visti, di spartire la visibilità tra tutti i membri del team. In pratica, se qualcuno ci osserva, il più delle volte si trova dove non stiamo guardando.

## Comportamenti insoliti

**Il pedinatore professionista è quello che, mentre il bersaglio entra a comprarsi le sigarette dal tabaccaio, è capace di restare fermo e fare assolutamente niente; il dilettante tenterà a tutti i costi di darsi un contegno, così aumentando il rischio di essere riconosciuto.** I lamer si appoggiano con fare noncurante a un lampione, come nella vita non fa nessuno; guardano distrattamente vetrine di negozi che non c'entrano niente con il loro stile e il loro aspetto; si appoggiano a una panchina del parco invece di sedersi, o aprono il giornale come nessuno legge il giornale; ci sono anche quelli che guardano attraverso la porta del bar per tenere in vista il bersaglio, e magari i pedinatori fossero tutti così.

**Ecco come funziona essenzialmente la dinamica del pedinamento.** Per saperne di più, sul come pedinare ma soprattutto come evitare di essere pedinati, scrivete!


**Reed Wright**
reedwright@mail.inet.it


### PEDINAMENTO FAI DA TE

Qualche consiglio ulteriore per riconoscere un pedinatore si ricava dalla pagina http://www.localmotion.it/templar/pedinamento.htm e, più in generale, presso http://spynet.has.it.

Dossier: Spynet

# Spazzatura puzzolente



**Rispondiamo a chi ci chiede cosa fare contro lo spamming.**

**Dalla pornografia spacciata per gratuita, alle vantaggiose iniziative commerciali multilivello che di vantaggioso hanno solo i soldi per chi le ha inventate: non passa giorno che tra le e-mail che riceviamo non ci sia spazzatura promozionale simile a questa.** Ovviamente senza che noi abbiamo mai richiesto nulla di simile. E ci fanno perdere un sacco di tempo per scaricare, filtrare e spulciare i vari messaggi ricevuti alla desolata ricerca di quei pochi che ci interessano, dovendo per forza di cose trascorrere ore davanti al monitor solo per cancellare tutta la feccia che intasa le nostre caselle email.

Si chiama spam: il termine deriva dall'inglese "spiced ham", prosciutto speziato. Negli Stati Uniti è infatti diffuso un tipo di carne in scatola, prodotto da una azienda chiamata Hormel, che porta proprio il nome SPAM.

Il suo collegamento con le invadenti email che costantemente girano per la rete assillando milioni di utenti ha origini a dir poco fantasiose, come quella teoria che vede associato il concetto ad un famoso sketch dei Monty Python's, il quale descrive una scenetta in cui una coppia entra in un ristorante e si trova a sedere a fianco di una tavolata di simpatici individui ubriachi (con tanto di elmetti vichinghi in testa) che con il loro canto assillante, "spam, spam, spam!" coprono le voci dei due mentre stanno ordinando la cena, causando alla fine la resa dell'uomo, che capitolando ordinerà appunto lo spam. Ma l'ipotesi più accreditata è che la SPAM originale, la carne in scatola cremosa SPAM, sia perfetta per descrivere l'atto di spalmare di qua e di là ogni sorta di schifezze.

Sin dall'origine del termine, dunque, "spam" viene immediatamente identificato come diffusione fastidiosa e non gradita. E la diretta semplicità di questa cacofonia è quantomai azzeccata.

## >> Ormai deborda ovunque

Ma cosa accade in pratica? E' semplice: la rete offre un'incredibile opportunità di comunicazione, la possibilità di raggiungere milioni di utenti sparsi per il mondo in brevissimo tempo con un mezzo in continua espansione e di grande efficacia mediatica. Ne sanno qualcosa i primi avvocati americani che hanno fatto ampio uso dello spamming per rilanciare il loro studio, ottenendo un successo strepitoso e una denuncia seguita dalla chiusura del loro provider. Ma ormai il business era fatto, e l'era dello spamming aperta.

Il vecchio sistema dei volantini lasciati nella casella della posta si è adattato perfettamente alla rete, moltiplicandosi però in modo esorbitante: mandare migliaia e migliaia di email con costi praticamente nulli, e così, per gli spammers, non resta che acquisire il maggior numero di indirizzi di posta e lanciare con pochi click una mole devastante di messaggi promozionali.




http://www.euro.cauce.org/it, contro lo spamming.

Detta così potrebbe sembrare - e in un certo senso lo è - la semplice applicazione telematica del concetto dei volantini. C'è il fatto, però, che per fare questo paragone dovremmo immaginare dei volantini inviati a spese del destinatario: difatti chi riceve spam in modo massiccio non deve soltanto eliminare i messaggi che non gli interessano, ma perdere prima il proprio tempo e i propri soldi nello scaricarli. E ci sono persone che regolarmente devono chiudere un indirizzo di posta (che magari usano per lavoro) e aprirne un altro a causa di questa immensa mole di messaggi.

Il dibattito sull' "etica" dello spam è acceso, e anche se può sembrare incredibile, sono moltissimi gli spammer che vi partecipano asserendo che la loro attività si fonda sul principio di libertà di parola.

Non vogliamo entrare nel merito di queste discussioni: troppo sarebbe lo spazio richiesto e poche le conclusioni pratiche. Rimane da pensare, per esempio, a tutte quelle persone che ricevono quotidianamente email a chiaro contenuto pornografico delle quali non hanno mai fatto richiesta, e che magari si trovano a dover fronteggiare situazioni quantomeno imbarazzanti nel momento in cui si trovano a scaricare la posta sul lavoro...

## >> Ma chi diavolo c'è dietro?

Una delle domande che immediatamente ci si pone in merito allo spam è: "ma da dove arrivano tutte queste email? Chi le

manda?" Si tratta sia di aziende sia di privati: chiunque abbia pochi scrupoli e interesse a raggiungere con i suoi messaggi il maggior quantitativo di utenti possibile è un potenziale spammer.
Lo spam avviene principalmente via email, ma è da considerarsi tale anche tutta quella mole di messaggi non richiesti provenienti da chat, instant messanger, newsgroups e mailing list varie: bot che entrano in un canale IRC particolarmente popolato pubblicizzando qualche sito porno, messaggini ICQ che ci chiedono di raggiungere un url di video chat, webmaster che postano il link al proprio sito in cross post a centinaia di ng diversi.
Tuttavia, lo spam che maggiormente si avvicina a quello che in pratica rappresenta un vero e proprio furto di servizi è il classico invio di email non richieste. Il problema è ormai chiarito: adesso occorre difendersi.




**Tracciato! E adesso spedisco al provider che ti ha lasciato libero una bella segnalazione.**

La prima regola è quella che più spesso ricorre in rete: conoscere il proprio nemico. In che modo gli spammers sono arrivati in possesso del nostro indirizzo email? Che cosa vogliono da noi?

## >> Non aiutiamoli

Quello che con maggiore frequenza uno spammer cerca è un indirizzo email valido: ovvero un indirizzo che qualcuno utilizzi il più sovente possibile per inviare e ricevere posta. Questo è uno dei punti cruciali: lo spammer ha interesse unicamente che i propri messaggi vengano letti, non importa tanto da chi. E dunque la più frequente reazione di fronte allo spam è anche quella più sbagliata: mai rispondere, neppure inc****ti, a un messaggio di spam!

## ADESSO TI BECCO

```
Return-Path: <ux564pl@yahoo.com>
X-Original-To: redazione@hackerjournal.it
Delivered-To: redazione@hackerjournal.it
Received: from cdm-68-226-188-15.lkch.cox-internet.com (cdm-68-226-188-15.lkch.
cox-internet.com [68.226.188.15])
        by server.hackerjournal.it (Postfix) with SMTP id 3E104C769
        for <redazione@hackerjournal.it>; Fri, 19 Dec 2003 00:15:39 +0100 (CET)
Received: from [212.37.76.134] by cdm-68-226-188-15.lkch.cox-internet.com with
ESMTP id 35303398; Fri, 19 Dec 2003 02:32:16 +0500
Message-ID: <zk-7vwb6018$$-m14o@pt7.jlqthg>
From: "Ericka Williams" <ux564pl@yahoo.com>
Reply-To: "Ericka Williams" <ux564pl@yahoo.com>
To: redazione@hackerjournal.it
Subject: Zoloft.t Valium.m Vicodin.n Xanax.x tzbrmsvaotgrkahvp
Date: Fri, 19 Dec 03 02:32:16 GMT
X-Mailer: The Bat! (v1.52f) Business
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="0148.B.2F0A7D_62C9B."
X-Priority: 3
X-MSMail-Priority: Normal
```

Esaminando le intestazioni di un messaggio, si può individuare il server da cui è effettivamente partito. Qualsiasi client di posta permette di visualizzare l'header; per esempio, Outlook bisogna aprire il messaggio e andare alla voce Visualizza/opzioni… La prima parte delle intestazioni presenta tutto il percorso che il messaggio ha compiuto prima di arrivare al nostro client:

**Return-Path: <ux564pl@yahoo.com>**

Indica l'indirizzo email del mittente (ma potrebbe essere stato contraffatto) e in ogni caso, come detto nell'articolo, non è consigliabile rispondere a questo indirizzo. Indicheremmo allo spammer che il nostro indirizzo email è proprio attivo.
Tutta la sfilza di "Received", invece, indica da quali server di posta è transitato il messaggio:

**Received: from cdm-68-226-188-15.lkch.cox-internet.com (cdm-68-226-188-15.lkch.cox-internet.com [68.226.188.15])**

Questa è l'ultima riga della serie di campi Received, e mostra il primo passaggio dell'email. Facendo un traceroute o un whois proprio su 68.226.188.15 (tramite un database online come abbiamo citato nell'articolo), potremo ottenere informazioni importanti sul server che lo spammer ha utilizzato per inoltrare il proprio messaggio. In questo caso:

```
OrgName:    Cox Communications Inc.
OrgID:      CXA
Address:    1400 Lake Hearn Drive
City:       Atlanta
StateProv:  GA
PostalCode: 30319
Country:    US7
```

Una volta acquisita questa informazione, potremo rivolgerci all'apposito servizio di abuse che si occuperà di impedire allo spammer di inviare altri messaggi.
Se fosse impossibile risalire al server utilizzato dallo spammer, o se questo non prendesse in considerazione le nostre lamentele, bisognerà cercare un referente nel corpo stesso delle email, utilizzando il dominio del sito pubblicizzato. Da questo dominio, si può risalire al provider che ne effettua l'hosting attraverso il database di Network Solutions (www.netsol.com/cgi-bin/whois/whois) per i domini .com, .net e .org, e in quello del Nic (www.nic.it/RA/database/viaWhois.html) per i domini italiani.it o per tutti con http://ww1.arin.net/whois/




Che cosa vi fa venire in mente? Esatto! La posta elettronica.

Fare un reply a messaggi di spam equi0vale a confermare allo spammer che ci bombarda che il nostro è un indirizzo email attivo, e che i suoi maledetti messaggi vengono letti da qualcuno in carne e ossa. Esistono in rete persone senza scrupoli che collezionano liste di migliaia e migliaia di indirizzi email per poi rivenderli allo spammer di turno, e un indirizzo confermato come "attivo" perché siamo stati tanto ingenui da avere risposto, ha un prezzo decisamente più alto che uno non verificato.
Senza contare, poi, che qualsiasi insulto o minaccia risulterebbe perfettamente inutile: lo spammer è il primo a rendersi conto di essere molesto, e di certo non verrà toccato dalle nostre lamentele.
E' dunque poco sensato anche seguire le istruzioni che il più delle volte accompagnano i messaggi di spam: rispondere alla email di turno inserendo "CANCEL" nel soggetto o altro non servirà a cancellare il nostro indirizzo dalle liste degli spammers: quello che vogliono è solo la certezza di inviare messaggi a qualcuno che li legge, e tutte le finte istruzioni che vengono poste in fondo ai messaggi per "cancellarsi da questa lista" servono solo a compilare altre liste di indirizzi email "certificati" che gireranno sempre più massicciamente tra le mani degli spammers.
La prima regola da seguire, quindi, è quella del silenzio e della pazienza. Perdere il controllo non serve a nulla, tanto più che nella stragrande maggioranza dei casi l'indirizzo email dello spammer risultante dagli header delle email non risulterà valido, o sarà di qualcuno che non c'entra nulla con lo spam in questione.
Quello che però è importante tenere a mente è sempre il fine ultimo di un messaggio di spam: nel 99% dei casi spillare soldi a qualcuno.
E dunque, leggendo i messaggi, potremo in ogni caso ottenere informazioni su chi ci sta contattando e perché. Quello di cui abbiamo bisogno per difenderci è un referente.

## >> Filtriamo tutto

A questo punto in molti si staranno chiedendo se non valga la pena di impostare dei semplici filtri sulla propria casella di posta: questo tipo di soluzione risulta efficace solo in parte, anche in considerazione del fatto che in ogni caso viene generato del traffico (che sia determinato dal download dei messaggi da parte del nostro client di posta o che i filtri vengano applicati dal server); il punto rimane quello di eliminare questo tipo di attività alla radice, dissuadendo l'invio non autorizzato di messaggi tramite un dialogo costante non con gli spammers, quanto con chi offre loro determinati servizi, in primo luogo quello di email.
Le operazioni da compiere quando riceviamo spam sono dunque innanzitutto cercare un referente (che comunque sarà indicato nel corpo del messaggio, sia esso un'azienda, un sito o una persona fisica); occorre in seguito identificare il provider a cui si appoggia lo spammer in questione: ciò può essere fatto andando a spulciare tra gli header della email, dai quali otterremo l'IP dello spammer ma, cosa più importante, anche i dati di chi gli fornisce la connettività.
E proprio a questo dovremo fare riferimento, andando a verificare da dove arriva lo spam e chi lo veicola.
Un qualsiasi sito dal quale fare whois (http://www.cgil.it/cesi/HotLinks/HotLinks-DNS.htm#whois) ci fornirà tutte le informazioni di cui abbiamo bisogno.
Una volta ottenuti gli estremi del provider utilizzato dallo spammer per inoltrare la sua sgradita corrispondenza, non dovremo fare altro che segnalare al provider stesso la presenza dello spammer. Molti provider, normalmente, hanno indirizzi appositi a cui inoltrare segnalazioni di spam (del tipo abuse@provider.it) e in genere, sia per una questione di traffico generato che di immagine, i grandi provider tendono a reprimere il fenomeno. Libero.it è piuttosto puntuale a riguardo, mentre tin.it si è mossa solo di recente.
La prassi da adottare è dunque quella di protestare "alla radice", evitando il contatto diretto con gli spammer, che non vedono l'ora di poter compilare liste chilometriche di indirizzi email che corrispondano agli ingenui.

# NEWS

## GUANTI DI LUCE

**Nessuno ha ancora inventato qualcosa che sostituisca davvero la combinazione di mouse e tastiera,** ma in molti ci provano e uno dei risultati più suggestivi è il Lightglove (http://www.lightglove.com). Somiglia a un orologio da polso con un cinturino piuttosto largo e riconosce il movimento e la posizione della mano e delle dita proiettando intorno a esse una sorta di guanto virtuale, fatto di luce. La mano e le dita, muovendosi, intersecano i raggi



di luce e il Lightglove interpreta i segnali corrispondenti perché corrispondano alla pressione di un "tasto" o al movimento del puntatore del mouse. Il concetto del Lightglove esiste da alcuni anni ma solo ora i progressi dell'hardware e del software permettono di pensare a unità affidabili e realmente utilizzabili.
Tra qualche anno potremmo trovarci tutti a digitare a mezz'aria… e sarà ben più difficile di adesso scoprire una password digitata da una centralinista distratta.



# GENOCIDE: PARTICOLARMENTE

**Una casa senza corrente, ma tanta dedizione agli impegni di ogni tipo. E una strada di hacker che inizia sui banchi di scuola...**

**E' lui? Non è lui? Un po' di mistero avvolge sempre le figure che hanno fatto la storia dei gruppi hacker più famosi.**

**È questa una storia particolare, di un ragazzo dell'Alaska che vive in una baracca senza elettricità e acqua corrente.** Fairbanks, questa la cittadina, è accogliente. Genocide, il teenager che stiamo prendendo in esame, è molto sveglio, dotato di una grande dedizione in tutto ciò che fa, attaccato alla famiglia e ai veri valori umani, insomma un ragazzo più che normale. Genocide: a proposito non abbiamo riflettuto sul nome. Ovviamente è uno pseudonimo, ma di quelli particolari, che ha alle spalle un lungo ma apprezzabile ragionamento. Non nasce infatti da un'idea cattiva di fronte all'argomento ("genocidio") quanto all'aspra critica che il ragazzo rivendica nei confronti di questo tipo di azioni criminose e nella violenza in generale: una scelta, lo ripetiamo, particolare, suggestiva e definitiva (nel senso che sarà lo pseudonimo che firmerà ogni azione del teenager).
Per sottolineare la normalità di Genocide, possiamo aggiungere che ha degli amici, studia con interesse, frequenta bar e pub (non che ce ne fossero molti a Fairbanks) e pratica sport, il wrestling. Insomma tutti aspetti che non combaciano con un nerd. Sebbene il ragazzo fosse attaccato alla famiglia, questa invece seguiva la scia negativa del periodo: il divorzio. Questo fatto anziché aggravare lo stato d'animo di Genocide, che aveva soli 5 anni, lo temprò nell'animo facendolo crescere, in fatto di responsabilità e dedizione, più veloce del previsto.
A scuola, abbiamo già accennato, Genocide non se la cava molto bene tranne che per la matematica e l'informatica: nonostante non avesse nemmeno l'elettricità a casa, il computer lo intrigava tantissimo sino a giungere a essere considerato un mago.
Il computer per Genocide risultò essere una "chiave verso l'ignoto", un modo per infrangere certe regole e limiti che obbediscono a leggi di un altro mondo, quello digitale. E infrangere i limiti diventò un impegno costante che si tradusse poi in un ossessione.



**Defcon: un appuntamento essenziale per il gruppo. Una serie di incontri decisivi per allargare amicizie e conoscenze.**

## >> Gli esordi

All'inizio di questa carriera, che possiamo già definire da hacker, gli esperimenti di Genocide sono per lo più dei giochetti, degli scherzi con cui poter seminare il caos nella rete scolastica. Tutto finisce lì: anzi è un gran bel divertimento. Prima semina il caos, poi gli insegnanti chiedono il suo aiuto perché i computer hanno un problema: Genocide mette tutto in ordine in cinque minuti. E' il genio ma soprattutto, nessuno lo sa ancora, oltre a essere lui stesso il responsabile di quei problemi, ha già raggiunto poteri da SysAdmin, ovvero il padrone indiscusso della rete scolastica: prima grande conquista.
Le sue capacità sono ben conosciute in giro, anzi proprio così riesce a stringere numerosi altri rapporti. Visto che la sua "attività" va bene, ciò lo rende soddisfatto e gli frutta anche alcuni onori, decide di pigiare sull'acceleratore: è in questo momento che nasce in lui la consapevolezza di tentare di divenire un hacker.
Inizia quindi, il teenager, ad acquisire nozioni di phraeking. Le lezioni sono gentilmente offerte da alcuni suoi cugini e amici "particolari". Nasce ufficialmente l'hacker Genocide. Per la verità, il suo curriculum non dice molto in quanto a phraeking, invece ci tramanda significativi exploit: quello per esempio, ed è un classico, del cambio di voto. Mancano infatti poche settimane al diploma e Genocide ha un problema con la chimica: il suo voto è insufficiente e così rischia di essere rimandato. Dopo aver accuratamente ispezionato lo user e password del suo docente di chimica, una mattina entra in aula informatica e si siede davanti a un Mac. Si collega, si cambia il voto: il diploma adesso è assicurato. Certo non è un gran

# UN RAGAZZO PREZIOSO

che come exploit, ma è il primo e va quindi menzionato. Più tardi, intraprende l'arte del cracking con lo scopo inizialmente di gabbare le password dell'intera rete e quindi di girovagare come una divinità per i computer e gli account di alunni e docenti. Il problema nasce quando l'amministratore scopre attivo un programma illegale: gli basta poco per capire da quale computer proviene. Non è difficile intuire che a quel computer siede Genocide. Riesce a intuire il pericolo e immediatamente lascia il computer cedendolo a un altro ragazzo e fugge via. Il tempismo è da oscar, l'adrenalina è alle stelle. Lo sfortunato studente si difenderà dai rimproveri dell'amministratore, ma Genocide è al sicuro.

Fairbanks diventa quindi un campo di addestramento importantissimo per il neohacker. Intanto il nostro inizia a prendere più confidenza con altri ragazzi che condividono la stessa passione per il computer: niente di strano. Se però ci aggiungiamo che tutti e cinque (compreso Genocide) hanno acquisito capacità di hacker, possiamo capire che gruppo di stia formando. WiZDom, Astroboy, Alexu e Malcom insieme a Genocide frequentano ormai regolarmente l'aula informatica e iniziano a scambiarsi alcune conoscenze.

Come ogni gruppo hacker che si rispetti, iniziano le gare dei virus, dei worm, insomma di hacking leggero: tutto per testare ognuno le proprie capacità rispetto agli altri membri. Genocide non sta più nella pelle. La madre, venendo incontro ad alcune richieste del figlio, riesce a connettere la "baracca" alla rete elettrica e telefonica e finalmente giunge a casa un Pentium 75Mhz. In concomitanza con questo avvenimento, nasce ufficialmente il gruppo Genocide2600 che avvia riunioni e progetti inerenti l'informatica e l'hacking.

Riescono, i cinque, a utilizzare come centro di attività un'aula dell'università. Attorno a queste riunioni un alone di successo: tanti partecipanti, tanti interventi, addirittura la presenza di qualche docente. Visto l'andazzo, i cinque del 2600 decidono di creare del materiale utile che distribuiscono su vari supporti (questo frutta qualche soldo) e prende vita il sito Genocide2600.com dove vengono raccolti materiale documentario, manuali, articoli, software… A livello locale, il gruppo 2600 è famoso.

## L'FBI

Come tutte le belle storie di hacking, non può mancare l'FBI. Durante una delle tante esplorazioni per il web, Genocide scopre e viola un sito: quello che riesce a raccogliere è materiale top secret. Megabyte di software sperimentale che serve per attaccare siti e quindi testarne la sicurezza. Ci sono pure dei documenti circa nuove falle nei sistemi operativi: in mano a un hacker quella era la chiave di tutto il mondo digitale. Con una scoperta ops…, con una hackerata di quel tipo, Genocide2600 divenne famosissimo: la portata dell'exploit è terrificante. Pochi giorni dopo, Genocide,



L'attuale pagina del sito Genocide2600.com

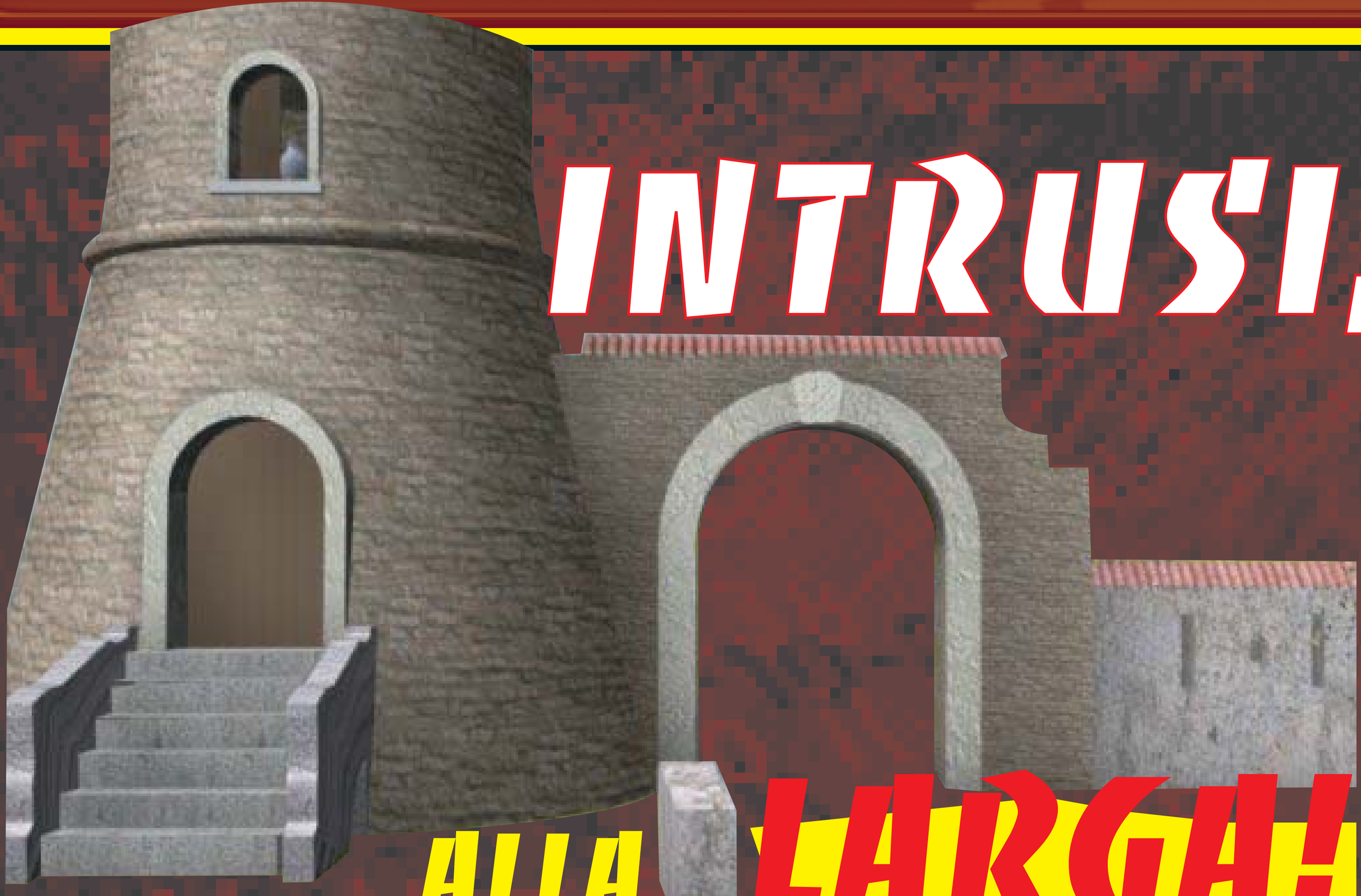
alla fine di un suo intervento in una riunione, viene affiancato da un uomo che gli mostra il tesserino dell'FBI: l'attacco è stato scoperto. Genocide riesce a mantenere la calma e capisce, da quel poco, che l'agente non è sicurissimo della paternalità dell'attacco e quindi la sua è un'azione intimidatoria. Comunque è un duro colpo . Le mosse da fare sono necessariamente due: fare sparire tutto il materiale "raccolto" e soprattutto le tracce dell'exploit dalla rete. L'FBI e l'Università, nonostante strazianti cyber-ricerche non riusciranno a incastrare Genocide e il suo gruppo. Ragazzini sì, ma nessuno ricorda che sono anche splendidi hacker.

Il triste avvenimento minò la compattezza del gruppo e delle riunioni: si perse grinta e continuità. Nel mondo digitale invece, le cose vanno decisamente meglio. Le capacità di Genocide sono notevoli, e il fatto stesso di aver eluso le ricerche dell'FBI è un elemento di analisi importante.

Oltretutto, il misfatto, accresce in lui un'idea precisa, che è il fulcro dell'etica hacker: tutto deve basarsi sulla condivisione delle conoscenze, e il principio fondamentale non può essere altro che la libertà d'informazione. Per rispettare il volere di Genocide, evitiamo di continuare nella trattazione degli altri exploit, ma precisiamo quanto segue: il ragazzo senza elettricità, col computer ci sapeva fare; con forza di volontà e dedizione ha saputo superare molte difficoltà; è andato incontro a scelte difficili, ha passato qualche guaio; ma è stato sempre mosso dall'etica positiva dell'hacker. Oggi è, a 26 anni, un prodotto dell'hacker esperto che era, con tutte le cicatrici.

"Sono solo un ragazzo che si occupa di sicurezza" – particolarmente prezioso – aggiungiamo noi.

**Francesco "KikoGeek" Corsentino**



# INTRUSI, ALLA LARGA!

**Non è difficile difendere il nostro computer dalle visite indesiderate di malintenzionati e script kiddy pasticcioni; a volte basta un programmino. Come questo**

**Soprattutto chi è sempre collegato a Internet, via FastWeb o ADSL, avrà certamente constatato come il suo computer subisce quotidianamente numerose scansioni da parte di programmi che cercano una porta aperta per entrare e fare festa senza avere l'invito.** Nelle prossime righe si spiegherà come realizzare e applicare un servizio che ascolta che cosa succede sulle porte e logga chi cerca di connettersi alla vostra macchina, con la possibilità aggiuntiva di bloccare il client che l'intruso sta utilizzando nel caso in cui avvenga una richiesta di connessione con invio di flag TCP "SYN". Nella pratica, qualora rilevasse una richiesta di connessione su una determinata porta selezionata da noi, il servizio invierà un flood testuale paralizzando momentaneamente il client, che si troverà a ricevere una grande mole di dati.
Ciò può essere molto utile per scoraggiare eventuali lamer che decidessero di tentare connessioni a porte particolarmente sensibili e che non corrispondono a servizi effettivamente attivi. Per esempio, chi installa un Web server locale non ha alcun bisogno dei servizi ftp (porta 21) o telnet (porta 23), e può quindi "proteggerli" con questo programmino.

## Facile con Visual Basic

Per realizzare questo programma serve l'ambiente di sviluppo Visual Basic, in versione 5 o 6. Create un nuovo programma .exe standard con un form nel quale inserirete una TextBox, una ListBox, 2 CommandButton e il winsock. Per rendere il tutto meno complicato e quindi l'algoritmo più comprensibile, eviteremo di inserire istruzioni di debugging come GestError e moduli di gestione dei controlli grafici (Enabled e altri).

**I componenti del programma sono:**

| OGGETTO | NOME |
|---|---|
| - Textbox | txtport |
| - Command1 | cmdascolta |
| - Command2 | cmddisconnetti |
| - List1 | lstlog |
| - Winsock | ws |

Potete vedere l'intero codice del programma nel riquadro in questa pagina. Passiamo quindi ad analizzare quello che abbiamo codato, analizzando uno per uno i suoi tre eventi: cmdascolta_Click (ciò che succede quando facciamo clic sul pulsante cmdascolta), ws_ConnectionRequest (ciò che succede quando riceviamo una richiesta di connessione dall'esterno) e cmddisconnetti_Click (ciò che succede quando facciamo clic sul pulsante cmddisconnetti).

### DEFINIZIONI:

**LOGGARE:** registrare gli eventi in un documento, detto log. In un log di connessioni Internet compaiono tipicamente dati come l'indirizzo IP del chiamante, la data e l'ora del collegamento.

**FLOOD:** grande quantità di dati inviata verso un computer o un programma, allo scopo di paralizzarne la connessione. Usato spesso per portare un attacco DoS, Denial of Service, in cui il server non è più in grado di rispondere.

## 1. cmdascolta_Click

```
Private Sub cmdascolta_Click()
ws.LocalPort = txtport.Text
ws.Listen
MsgBox "Servizio in ascolto sulla porta: "& txtport.Text, vbInformation
End Sub
```

Come dicevamo, questo è quanto accade quando si fa clic sul CommandButton "cmdascolta". Come prima cosa istruiamo il nostro ws per impostare come porta locale la porta che viene scritta nella txtport "txtport.txt <— testo della txtport", gli ordiniamo di mettersi in ascolto su quella porta e infine di visualizzare una finestra msgbox "messaggio" con scritto:

**"Servizio in ascolto sulla porta: " & txtport.Text," dove appunto**

```
"& txtport.Text"
```

indica l'immissione nel messaggio del numero digitato nella txtport.
"Vbinformation" indica il tipo di msgbox, nel nostro caso informazione\notifica



Sottoposto a un attacco flood, un client si blocca e non riesce a più procedere.

## 2. ws_ConnectionRequest

```
Private Sub ws_ConnectionRequest(ByVal requestID As Long)
If ws.State <> sckClosed Then ws.Close
ws.Accept requestID
lstlog.AddItem "Connessione di :" & ws.RemoteHostIP & " sulla porta :" & txtport.Text
For i = 1 To 10000
ws.SendData "Sei stato loggato, sparisci lamer —> " & ws.RemoteHostIP & vbCrLf
Next i
End Sub
```

Ora analizziamo invece quanto avviene nel caso in cui il nostro servizio riceva una richiesta di connessione "ricezione flag TCP SYN". Come prima cosa accetta la connessione, in seguito aggiunge una riga al log "lstlog" inserendo un messaggio del tipo

**"Connessione di : *ip del lamah" sulla porta : *scritta nella txtport*"**

Dato che ws.remoteHostIp indica l'IP dell'host remoto che cerca di connettersi, una volta accettata la connessione e loggato l'indirizzo del lamer si attiva il ciclo di for "impostabile", ossia:

```
ws.SendData " Sei stato loggato, sparisci lamer —-> " & ws.RemoteHostIP & vbCrLf
```

che indica un invio di diecimila stringhe, con il comando
Questa stringa verà visualizzata dal lamer che cerca di connettersi e invece leggerà il FuckMsg (messaggio di vaffa) con accanto il suo IP. Il vbCrLf alla fine della stringa la manda a capo, facendo in modo che le scritte ripetute non si sovrappongano una sull'altra, ma vengano visualizzate belle leggibili in colonna,

```
For i = 1 To 10000
ws.SendData " Sei stato loggato, sparisci lamer —-> " & ws.RemoteHostIP & vbCrLf
Next i
```

# NEWS

## CHI COPIA PAGA!

**SPX e la sua unità Imagexpo hanno annunciato che Microsoft pagherà 62,5 milioni di dollaruzzi di danni per avere violato un brevetto nella creazione di NetMeeting.** Il brevetto è esattamente il numero 5.206.934 e copre gli "apparati e i metodi per la videoconferenza interattiva tra computer". La corte della Virginia ha condannato Microsoft il 14 novembre scorso ma le parti sembrano avere raggiunto un accordo. Può darsi che la cifra alla fine sia leggermente inferiore, ma anche stavolta Microsoft se la caverà pagando per quello che ha rubato. Certo, è poca roba rispetto ai 521 milioni di dollari che Microsoft è stata per ora condannata a sborsare in agosto per compensare l'University of California ed Eolas Technology per violazione di un brevetto sull'uso di plugin per browser e ai 750 milioni di dollari pagati in maggio a Time Warner per un'altra causa, ma il principio sembra reggere: chi ruba, se non altro, paga. Prima o poi riusciranno anche a farla smettere di rubare.

## WELCOME LORMA LINUX

**È arrivata Lorma Linux 4.0, distribuzione basata sul core Fedora, come Red Hat,** ma dedicata in special modo a studenti e università. Lorma Linux 4 è composta da un solo CD, solo il software essenziale, e consente, con lo Scenario Chooser, di scegliere tra più configurazioni che semplificano la vita del non esperto e permettono di allestire rapidamente la configurazione migliore possibile per le proprie necessità. C'è tutto quanto serve per usare Internet al meglio, masterizzare, leggere DivX e vedere le animazioni Flash (sigh), ma manca il supporto di Java, non per incapacità realizzativa quanto per mancanza di spazio. Chi ne sentirà la mancanza potrà comunque richiedere un CD supplementare oppure andare a recuperare tutto ciò che gli serve sul sito della distro, http://linux.lorma.edu.

## NEWS

### SP2, BETA1

**Ha passato il primo stadio di beta il Service Pack 2 di Windows, XP, numero di build 5.1.2600.2055.** Se li trovate ancora (non dureranno, penso), ci sono degli screenshot su http://www.neowin.net. Dal canto suo Microsoft ha reso nota la documentazione di tutti i cambiamenti apportati alla beta, che potete trovare al comodissimo link http://download.microsoft.com/download/8/7/9/879a7b46-5ddb-4a82-b64d-64e791b3c9ae/WinXPSP2_Documentation.doc.

### AUSTIN SCEGLIE LINUX

**La capitale del Texas non è San Antonio o El Paso, ma Austin. E ad Austin, da qui a un anno, non si userà più Windows ma Linux.** La municipalità ha infatti annunciato che a fine 2004, alla scadenza dell'attuale contratto con Microsoft, la maggioranza dei 5.200 computer presenti nei suoi uffici sarà già passata al pinguino più libero del mondo. Secondo gli analisti la città risparmierà, con questa mossa, la bazzecola di tre milioni di dollari, e scusate se è poco.

sul client telnet di chi cerca di connettersi. Il numero di ripetizioni può essere modificato a piacimento. Impostando un numero molto alto di ripetizioni (come 500.000) si potrà impallare il client che "l'utente" sta usando per connettersi, costringendolo quindi a killare il processo. Ciò funge anche con client che non visualizzano i dati ricevuti, come per esempio alcuni portscanner, client ftp o, perché no, WebCracker e company, i quali andranno solo in overflow bloccandosi. Se invece non desideriamo eseguire l'attacco, ma solo far visualizzare a chi si connette il "messaggio di benvenuto" e loggarlo, ci basterà eliminare il ciclo di for nel quale è inserita la stringa da inviare, ossia eliminare

```
For i = 1 to 10000
```

e anche

```
Next i
```

lasciando quindi solo la stringa da inviare. Se invece non desideriamo far visualizzare a chi si connette alcun messaggio, optando quindi solo di loggare il suo IP, dobbiamo eliminare anche

```
ws.SendData "Sei stato loggato, sparisci lamer --> " & ws.RemoteHostIP & vbCrLf
```

facendo inmodo che il socket ws non invii nulla.

### 3. cmddisconnetti_Click

```
Private Sub cmddisconnetti_Click()
ws.Close
MsgBox "Sessione terminata", vbInformation
End Sub
```

Questo invece è quanto accade cliccando sul CommandButton "cmddisconnetti". Come prima cosa verrà



chiuso il socket, e quindi il programma non sarà più in ascolto. In seguito verrà visualizzata una msgbox "messaggio" con scritto "sessione terminata", di tipo vbinformationì "informazione/notifica". Il programma si conclude qui. Se desiderate avere il programma in ascolto su più porte diverse, basterà impiantare tanti sock quante sono le porte da tenere in ascolto.

## IL CODICE DEL PROGRAMMA LISTENING

```
ws.LocalPort = txtport.Text
ws.Listen
MsgBox "Servizio in ascolto sulla porta: " & txtport.Text, vbInformation
End Sub
Private Sub cmddisconnetti_Click()
ws.Close
MsgBox "Sessione terminata", vbInformation
End Sub
Private Sub ws_ConnectionRequest(ByVal requestID As Long)
If ws.State <> sckClosed Then ws.Close
ws.Accept requestID
lstlog.AddItem "Connessione di :" & ws.RemoteHostIP & " sulla porta :" & txtport.Text
For i = 1 To 10000
ws.SendData "Sei stato loggato, sparisci lamer --> " & ws.RemoteHostIP & vbCrLf
Next i
End Sub
```

HACKER JOURNAL

Anno 3 - N. 42
15 Gennaio 2004 - 29 Gennaio 2004

Direttore Responsabile: Luca Sprea

I Ragazzi della redazione europea:
grand@hackerjournal.it, Il Coccia, Gualtiero Tronconi, Ana Esteban, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Brugu s, Gregory Peron

Service: Cometa s.a.s.

DTP: Davide F0█ Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Eugenio Spagnolini

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Roto 2000

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.



**HJ: INTASATE LE NOSTRE CASELLE**

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. redazione@hackerjournal.it

## hack·er (hãk'∂r)

***"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."***

# SICURAMENTE INSICURI

**Gennaro ci ha mandato una mail che per noi merita l'editoriale. L'abbiamo riassunta per motivi di spazio, ma lasciando invariate le sue argomentazioni. Discutiamone.**

Si parla di sicurezza, di leggi che puniscono gli hacker e di buchi clamorosi in S.O. blasonati. Non si fa però mai cenno alle falle di sicurezza dovute a incuria e inesperienza (e incompetenza) di coloro che dovrebbero essere gli esperti. Pagati fior di quattrini e che spesso dovrebbero essere proprio loro a risarcire i danni alle società colpite, vista la loro imperizia.

A cosa servono i software per la scansione delle chiavi quando le password sono quelle preimpostate in fabbrica? Non mi è mai capitato di trovare un router ADSL su cui qualcuno si sia preoccupato di modificare la chiave di amministratore preimpostata in fabbrica, facilmente scaricabile e in bella mostra nel manuale in linea del router. Che magari è user: Admin e pw: Admin!

Ancor meno frequente è vedere qualcuno che si assicuri di dare agli utenti della rete accesso limitato ai soli servizi http e https. Poi, su richiesta del collega amico che deve scaricare l'ultimo album del suo cantante preferito, si aprono falle su tutto il sistema.

A proposito di peer to peer: quanto pensate che occorra a un manipolo di malintenzionati per creare una piccola rete p2p e che un software ad hoc per tale rete trasformi i pc delle vittime in proxy per dare ai malintenzionati una sicurezza di anonimato? Molto poco! Una decina di CD trendy e cinque o sei pc in rete.

Chi immagina di utilizzare un pc da rottamare come router/firewall tra due sottoreti della propria intranet in modo che una sottorete, magari aperta al pubblico, non possa accedere alla restante rete in cui sono registrati dati sensibili?

Quanti usano la possibilità di criptare intere parti dell'hard disk fidandosi ciecamente dell'antifurto installato (a cui non è stato modificato il codice di accesso preimpostato in fabbrica :-)? Abbiamo segnalato al servizio assistenza che sul nostro disco ci sono dati sensibili, per cui vanno prese determinate precauzioni in caso di sostituzione del disco stesso?

E se dal pollo arriva lo studentello sventolando un floppy, che chiede: "mi fa inviare questo testo al mio amico? Il mio modem si è rotto!"? Il pollo educatamente si sposta per non leggere la posta e lo studentello gli installa un trojan!

Quanti, dopo aver annotato una password su un foglietto, lo distruggono?

La notte chiudiamo il pc in cassaforte ignifuga, di giorno lo circondiamo di filo spinato. Eppure non abbiamo considerato che il Capo, portatosi il lavoro a casa, ignora che un'ora prima suo figlio dodicenne, attirato da una pubblicità ingannevole su un sito innocuo, ha infettato il pc del padre di virus che a loro volta hanno infettato il floppy su cui è stata scritta la relazione e di lì il pc del capo in ufficio.

Qualche apprendista stregone ha già pensato di far comprare al capo un portatile (tanto lui di soldi ne ha) e di aver messo in sicurezza la propria rete dimenticando che il collega a cui ha negato il p2p per scaricare l'ultima compilation di grido, rivolgendosi all'amico del cugino del cognato del fidanzato della figlia, si è fatto spiegare come installare un tunnel http.

Dobbiamo rassegnarci a tutta questa insicurezza?

Purtroppo sì! A meno che non si voglia tornare alle schede perforate (e qualche volta le rimpiango) oppure, molto più "semplicemente", lasciare fare ai veri esperti di sicurezza. Quelli che considerano la loro postazione uno strumento di lavoro e non un giocattolo e sono capaci di eliminare tutti quei servizi di cui non si ha bisogno, per vivere tranquilli e sicuri di essere insicuri :-)

**Gennaro Gaglione**

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

HACKER JOURNAL

## mailto:
redazione@hackerjournal.it

### GOOGLEWHACK UNO

Ciao,
puoi spiegarmi meglio di cosa si tratta, ho letto su hacker journal [numero 40, Draghi di Google. N.d.B.], puoi farmi un esempio di come sia possibile trovarli? grazie…

**Gick**

*Ciao Gick, guarda qui sotto!*

---

### GOOGLEWHACK DUE

A proposito di Googlewhack, che ne pensi di Menestrelli Sovrumani, oppure Armadilli Scontati, oppure Girogiostra Fulgente, oppure Sagrati Rampanti, oppure Incorporeità Incompresa? Li ho cercati in maniera tale da avere un suono decente, che potessero suonare come se li usassimo tutti i giorni. Spero li pubblicherete, è stato molto divertente!

**Bladefun**

*Li pubblichiamo sì, perché sono davvero carini!*
*A grande richiesta ripubblichiamo qui sotto una sintesi del testo del numero 40 dove Reed Wright spiegava il Googlewhack:*
*Un Googlewhack è una ricerca su Google, rigorosamente di due parole, che dà come risultato uno e un solo sito. Trovare Googlewhack non è difficile ma neanche facile ed è difficile fare esempi, perché nel momento stesso in cui si trova un Googlewhack è probabile che poco dopo non valga più, magari perché i risultati diventano due: il Googlewhack e la pagina di uno che segnala il Googlewhack, e cose così. Però nel momento in cui scrivo questo articolo "senectute immantinente" è un Googlewhack [lo è ancora. N.d.B.]. Ci sono delle regole: non vale usare le virgolette, le parole devono essere di uso comune (niente nomi propri, niente parole inventate) e il risultato non è valido se consiste nel link a una pagina di una lista di parole (come un dizionario o un glossario). Se trovate un Googlewhack lo pubblichiamo, sulla rivista o sul sito! E poi speditelo anche a www.googlewhack.com, dove li raccolgono. Qualche vero hacker sarà capace di scrivere un programmino Perl, o altro, che va in cerca di Googlewhack. Lo aspetto al varco!*
***Vale ancora. Chi trova Googlewhack belli come questi, o di più? Qualcuno è capace di fare il programmino? Chi scopre le varianti del gioco? Siamo***

googlewhack
The Search for "The One"

***qua!***

---

### REGEX UNO

Non ho capito bene cosa siano queste espressioni e come possano essere utilizzate. Vorrei anche chiederti dove posso trovare documentazione buona su queste cose e soprattutto di come si possano implementare in Java.

**Daniele.**

*Per il momento mi limito a dirti di fare una ricerca su Google della parola regex e di visitare, per Java, http://regex.info. Poi, leggi qui sotto. :-)*

---

### REGEX DUE

Ciao, […] ho trovato la semplice soluzione del secondo caso, ma mi riesce difficile trovare quella per il terzo e mi sorgono alcune domande: non c'è un'istruzione che non dà dei parametri come [0,9] ma dice "prendi il pezzo della stringa fino a che trovi il carattere…"?

**LoRd_MoRo**

*Ciao, guarda qui sotto!*

---

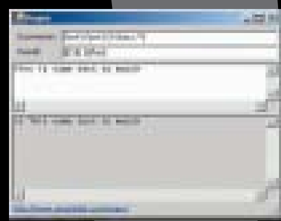
### REGEX TRE

Ciao Barg,
Ti scrivo perché [complimenti] il tuo articolo sul #40 […] rispondo alle tue domande: […] Comunque volevo farti anche una precisazione sul 1° problema da te risolto... in realtà la tua soluzione \d{2}\d?\d?[/,;@#-]?\d{5}\d?\d?\d? è sì in grado di riconoscere tutti i numeri di telefono italiani validi, ma non SOLO i validi […] il mio problema è molto semplice: estrarre tutte le Email di una certa "cartella" da Outlook Express in modo da salvarle in un formato diverso [eml, doc, xml, html, …). […] non mi era venuto in mente che avrei potuto scrivere io il tool in questione usando java con JLex e Cup… sono proprio pigro! ;-)

**Jerk**
**jerk@hackerjournal.it**

*Ciao Jerk!*

*Ho molto riassunto la tua mail e quelle prima (compresi tutti gli altri che hanno scritto, da Roberto Bossola in poi) perché qui nella posta non abbiamo spazio a sufficienza per approfondire la questione. Ma è per dire che lo farò in un prossimo articolo, con tutto lo spazio che serve e con tutte le vostre soluzioni, proposte e domande. Il tema delle espressioni regolari è piaciuto e d'altronde l'articolo era a livelli elementari, quindi non poteva entrare nel merito di tutto. Si può dire molto di più e… lo faremo. Se qualcuno ha domande in merito si faccia pure avanti!*



---

### COME DIVENTARE HACKER

Vi scrivo per chiedervi come è possibile diventare un "hacker" (intendo un esperto di computer, non uno che rompe le scatole agli altri). Ho il mio primo pc da 4 mesi e ho comprato praticamente ogni tipo di rivista. L'impressione che se uno non ne sa non ne dovrà mai sapere mi è venuta dopo la prima pagina. Imparare a usare il pc senza sapere l inglese non e certo facile e complicare l'italiano con termini cifrati non mi aiuta, lo devo buttare? Posso trovare un manuale base con

# www.hackerjournal.it

dizionario? Voi cosa consigliereste a un alieno appena arrivato in questo mondo che vorrebbe usare un pc? Vi ringrazio anticipatamente per la pazienza sperando in una risposta positiva.




**Alessandro**

***Caro Alessandro,***
***non so da dove cominciare ma ci provo. Sono usciti numerosi libri negli ultimi mesi con titoli tipo "Il manuale del giovane hacker" e simili, ma non ti aiuteranno. L'hacker non compra un libro per diventare hacker; curiosa, si impegna, studia, prova, improvvisa, inventa fino a quando non può scriverne uno! Scherzo, ma non completamente. Sii curioso e cerca di andare sempre alla sostanza e al cuore delle cose e metà del lavoro l'hai fatta. Un esempio stupido ma per me coerente: che cos'è un byte? Un hacker si butta su it.wikipedia.org e trova la risposta. Un non hacker cerca un libro scritto da un hacker che lo spieghi… e ora tutta la verità, fino in fondo. L'esempio che ti ho fatto funziona anche in italiano. Ma l'inglese è indispensabile, non solo per fare l'hacker. Un consiglio: non prenderla come una lingua da imparare, ma come una sfida da affrontare. Scriviti tre, cinque, dieci vocaboli di inglese al giorno e imparali a memoria, ogni giorno tre/cinque/dieci vocaboli nuovi. Tempo sei mesi e ci darai lezioni a tutti. Quando sei in dubbio, scrivici.***

---

## FORSE TROPPO CONTROLLO

Gentile redazione,
volevo chiedervi, siccome da poco ho comprato un secondo pc per i miei figli, come poter controllarlo dalla mia macchina, e come loggare i siti da loro visitati, i programmi installati, i tasti digitati eccetera, e inviare tutto alla mia mail. Poiché non sono un esperto di linguaggi vi prego di indicarmi dei programmi per poterlo fare automaticamente. (La sicurezza passa anche di qua: vedere cosa fanno i propri figli col computer e quali siti visitano).

**Peppe**

***Gentile Peppe,***



***potrei consigliarti decine di keylogger (i programmi che loggano i tasti premuti) e altri programmi che fanno le cose che vuoi tu, ma non lo faccio, per due motivi. Primo: seguendo Hacker Journal e Hacker Magazine avrai già in casa un arsenale di software e di istruzioni. Secondo: penso che saresti molto più sicuro parlando con i tuoi figli, navigando insieme a loro e fidandoti. Pur sapendo che gli capiterà di sbagliare, e che sbagliare significa crescere. Non fosse altro che, se loro ne sanno più di te, tutti i tuoi keylogger risulteranno vani.***

---

## INTERCETTAZIONE GSM

Sono uno studente di ingegneria delle telecomunicazioni e vorrei sapere se conoscendo l'identificativo IMEI e/o il numero telefonico di telefonino sia possibile attraverso la rete e eventualmente con qualche altro apparato riuscire a localizzarlo (anche a breve raggio) o sapere il traffico in entrata e uscita.

**Lastangel83**

***Vedo poche possibilità.***
***L'IMEI non ti serve a niente per la pura localizzazione (al massimo è meglio avere uno scanner radio per captarne il***



***segnale quando chiama). Per quanto riguarda l'ascolto del traffico, non ti serve sapere l'IMEI quanto invece l'IMSI, immagazzinato sulla SIM, che contiene le informazioni dell'abbonato. A livello accademico il codice di cifratura GSM è stato violato, ma a livello di utilizzo pratico non è esattamente facile***

---

## WINDOWS 98 A TEMA

Ciao! […] Mi chiedevo se esiste un metodo o un programma per "emulare Windows XP" su Windows 95/98 in modo tale […] da far assomigliare il desktop a quello di Windows XP, cambiare l'aspetto delle finestre e della barra delle applicazioni e il menu d'avvio… In pratica usare Win 95/98 con le caratteristiche grafiche di XP.

**attashow**




***Ciao a te!***
***Puoi tranquillamente trovare un sacco di temi come quello che cerchi nei siti dedicati, per esempio http://www.aaa-themes.com/xpdesktopthemes.phtml. Stai attento ai siti che ti regalano il tema ma poi non ti mollano più e vogliono a tutti i costi una marea di dati per inviarti mail pubblicitarie.***

---

## POSTA DEL KAISER

cara redazione so gia che le mie parole non vi faranno minimamente riflettere comunque continuero nel mio intento che qualche cosa cambi. […] xke no cambiare nome alla rivista e chiamarla securitycomputerjournal siccome la state facendo diventare una rivista di sicurezza. […] x me i virus sono il tramite tra massmedia e l'hacker. […]
Poi la rivista è carina (si fa x dire) mancano troppe robe, guide al linguaggio c++, c, pascal, vb, ecc… in pratica programmazione, magari aggiungere sorgenti di programmi, virus (non quella sotto specie del primo numero), cosi che il lettore possa confrontarlo con i suoi sorgenti. Nella rivista mettere + hacker e - sicurezza […]
Ultime precisazioni il vostro sito fa schifo […]
Avrei piacere che ritoccaste questa lettera e la pubblicaste sul prossimo numero di hj con risposta inclusa. […]
ciao by



**kaiser741**

***Ciao kaiser!***
***Abbiamo sintetizzato la tua lettera, non***